



BIJLAGE A SPECIFICATIE VAN DE OPDRACHT

Europese aanbesteding

“IT Service Management-oplossing”

Versie : 1.2
Kenmerk : IUC 23-018
Datum : 17-09-2024

INHOUDSOPGAVE

Hoofdstuk 1. Inleiding	4
1.1. De IST-situatie	4
1.2. De SOLL-situatie.....	4
1.3. Offerteproces	6
1.4. Samenwerken conform Agile/ aanpak installatie, Inrichting en Migratie.....	7
Hoofdstuk 2. Functionals	9
2.1. Algemeen.....	9
2.2. Archiveren.....	9
2.3. Rapportage.....	9
2.4. Selfservice.....	10
2.5. Proces inrichting	11
2.6. Technische interface integratie.....	11
2.7. Koppelingen	11
2.8. Forum Standaardisatie	12
2.9. Eisen aan practices	13
Hoofdstuk 3. IV kaders	14
3.1. Non-functionals	14
3.2. Beveiliging	16
Hoofdstuk 4. Integriteit.....	26
4.1. Business Etiquette.....	26
Hoofdstuk 5. Maatschappelijk Verantwoord Inkopen (MVI)	27
5.1. Energie & Klimaat.....	27
5.2. Welzijn & Gezondheid	28
5.3. Social Return on Investment	28
5.4. Internationale sociale voorwaarden	29
Hoofdstuk 6. Juridische kaders	31
Hoofdstuk 7. Prijsstelling	32
7.1. Algemene eisen ten aanzien van Prijzen.....	32
7.2. Toelichting Prijscomponenten in Bijlage VIII "Prijzenformulier"	32
7.3. Specifieke eisen ten aanzien van Prijzen	34
7.4. Indexering Prijs	34
Hoofdstuk 8. Documentatie, Opleiding en Consultancy	36
8.1. Documentatie	36
8.2. Opleiding	36

8.3.	Consultancy	37
Hoofdstuk 9.	Beschikbaar stellen en Inrichten	38
9.1.	Inrichting en beschikbaarstelling	38
9.2.	Documentatie, Opleiding en Consultancy	39
9.3.	Voortbrenging van (onderdelen) van de ITSM-oplossing	39
Hoofdstuk 10.	Onderhoud & Support.....	40
10.1.	Onderhoud & Support.....	40
10.2.	Factureren en bestellen	44
10.3.	Kaders voor (re)transitie	45

Hoofdstuk 1. Inleiding

Dit document beschrijft de eisen en wensen die de Aanbestedende dienst stelt in het kader van de Europese aanbesteding met kenmerk IUC 23-018. Dit document maakt integraal onderdeel uit van het Beschrijvend Document versie 1.2.

In dit document zijn een aantal teksten blauw en groen gearceerd; deze dienen als extra hulp c.q. aandachtspunt.

De blauwe arcering betreffen Eisen waarop ook met NVT geantwoord mag worden; de groene arcering betreffen zaken die in het DAP moeten worden beschreven.

1.1. De IST-situatie

De huidige ITSM-oplossing is op basis van ITIL®3 voor de in paragraaf 2.5 van het Beschrijvend document versie 1.2 genoemde 14 practises en 6 integraties ingericht op basis van IBM ICD en Flexera. De geïmplementeerde practises hebben een wisselend volwassenheidsniveau en zijn in het verleden silomatisch opgezet. Inschrijver moet ervan uitgaan dat het in gebruik nemen en Migratie nog uitgezocht moet worden per practice hoe e.e.a. nu exact werkt en wat wel en wat niet zinvol is om over te nemen in de nieuwe oplossing.

Te migreren objecten voor IV:

Vanuit de huidige oplossing (ICD) moeten Gegevens van openstaande objecten naar de ITSM-oplossing gemigreerd worden. In Bijlage VIII Prijzenformulier versie 1.1, tabblad Dimensionering is hiervan een overzicht gegeven.

Het aangegeven aantal objecten is een momentopname.

1.2. De SOLL-situatie

De directie IV van de Belastingdienst heeft drie hoofddoelstellingen geformuleerd om samen met de business voor informatievoorziening te zorgen die bijdraagt aan een financieel gezond en veilig Nederland, te weten:

- Top 3 IT-werkgever van Nederland zijn voor engineers (bouwers): medewerkers zijn trots om voor IV te werken;
- Tijdige en kort-cyclische levering: features worden afgerond volgens met de business overeengekomen plannen en kennen een korte cycle time. De IV-oplossingen voldoen aan de vraag van de business;
- 99,9% beschikbaarheid: een grote mate van stabiliteit en continuïteit voor de business binnen service windows en een hoge standaard van cybersveiligheid.

De nieuwe ITSM-oplossing is randvoorwaardelijk voor bovengenoemde doelstellingen en levert hieraan een bijdrage door middel van:

- Sterk verbeterde gebruikers ervaring (selfservice portaal en chat robots);
- Reductie van manueel of herhaaldelijk werk (automatisering van workflow en taken het inzetten van Artificial Intelligence, mobiel benaderen van de ITSM oplossing;
- Efficiënter werken: meer doen met minder mensen;
- Meer verantwoordelijkheid naar de Eindgebruikers om zelf zaken op te (kunnen) lossen (door middel van API- toegang tot de ITSM-oplossing)
- Een eenduidige architectuur, die toekomstige ontwikkelingen als de beweging naar DevOps voortbrenging maximaal faciliteert en waarvan de onderhoudsinspanning minimaal is.

In de SOLL-situatie zijn de IT-beheerprocessen van de IV Organisatie van de Belastingdienst op basis van ITIL®4 ingericht.

De IT beheerprocessen worden ondersteund door de ITSM-oplossing, waarbij de Inrichting van de ITSM-oplossing zo dicht mogelijk bij de "out of the box" Inrichting van de Opdrachtnemer blijft.

Dit stelt Opdrachtgever in staat om beter in control te zijn over het voortbrengingsproces IV in termen van juiste, tijdige en efficiënte uitvoering.

Deze situatie wordt niet ineens bereikt, maar fasegewijs. Hiervoor zal een Roadmap worden opgesteld.

In de eerste fase zal het huidige tool, IBM Control Desk (ICD), worden vervangen. Dit betekent dat eerst alle IT-

beheerprocessen die de Opdrachtgever nu kent en geïmplementeerd zijn in ICD, in deze fase worden gemigreerd naar de nieuwe ITSM-oplossing. Uitgangspunt is dat we de practices van de Opdrachtnemer volgen en de onderlinge samenhang van de processen borgen.

In de huidige ITSM oplossing op basis van ICD zijn een aantal gegevens ondergebracht die als hoog vertrouwelijk zijn geclassificeerd (vanuit algemeen security perspectief) en zijn er een beperkt aantal bijzondere persoonsgegevens (IT-Arbo middelen) opgenomen. Tijdens de eerste fase zal met de Opdrachtnemer een afweging gemaakt worden of het inzetten van een private key van de Belastingdienst hiervoor een economisch verantwoorde oplossing is, dan wel dat het beter is deze gegevens buiten de nieuwe ITSM-oplossing te houden.

Naast de technische Inrichten van de ITSM-oplossing zullen gebruikers en organisatie meegenomen moeten worden in de veranderingen die worden doorgevoerd. Dit is geen onderdeel van deze aanbesteding.

Voor de volgende practices is de Inrichten ingevuld met een koppeling met bestaande producten:

- Monitoring en Event Management: koppelvlak met NetCool Operations Insight;
- IT Asset Management: koppelvlak met Flexera;
- Portfolio Management: koppelvlak met Fortes Change Cloud.

De SOLL-situatie voor de eerste fase is bereikt als:

- Genoemde eerste 14 practices en 6 integraties zijn Ingericht in de nieuwe ITSM-oplossing;
- De performance en de werking van de ITSM-oplossing is geaccepteerd door gebruikers;
- De Migratie van aangewezen gegevens is afgerond (zie voor aangewezen gegevens paragraaf 1.4);
- Eindgebruikers en Behandelaren de nieuwe ITSM-oplossing gebruiken;
- DevOps teams de mogelijkheid hebben om te integreren met de ITSM-oplossing;
- De oude ITSM-oplossing (ICD) niet meer gebruikt wordt en is uit gefaseerd;

Binnen de IV-organisatie wordt de verandering gestuurd door de IV-keten. De inrichting van de IV-keten op basis van SAFe Agile is nog maar net gestart. Bedoeling is dat er op termijn een Roadmap ligt met te realiseren epics/features. Daar kunnen ook verdere optimalisaties in zitten waarvoor de ITSM-oplossing nodig is, of waarvoor geïmplementeerde practices verder worden geoptimaliseerd. Het is denkbaar dat voor de realisatie van één van deze epics/features aanvullende practices nodig zijn.

1.2.1. De transitie naar de SOLL-situatie

De IV-organisatie zit in een meerjarige periode van strategische transitie naar een dienstverlenende organisatie die op Agile & DEVOPS wijze werkt en levert.

De IV-organisatie zet over een periode van meerdere jaren in op een transitie naar een Agile manier van werken en het verder automatiseren van de automatisering, waarbij de inrichting van DEVOPS een belangrijk onderdeel is.

Na de verwerving van de nieuwe ITSM-oplossing zal de besturing van de transitie van 'oud' naar 'nieuw' ITSM plaatsvinden vanuit een project aangestuurd door de IV-keten. De samenstelling van dit project is IV-breed.

De eerste transitiestap zal bestaan uit het zodanig configureren van de verworven ITSM-oplossing dat de huidige implementaties in ICD kunnen worden uit gefaseerd. Hierbij is het de bedoeling dat de nieuwe ITSM-oplossing zo wordt ingericht dat er een geïntegreerde oplossing staat die standaard (dus geen maatwerk) is ingericht. De ITSM-oplossing moet voorbereid zijn op de integratie van de ontwikkelomgeving die door DEVOPS teams worden gebruikt.

Met behulp van deze integratie moeten resultaten uit het DEVOPS proces worden geregistreerd in de ITSM-oplossing. Het is de bedoeling om de ITSM-oplossing door middel van zo klein mogelijke wijzigingen in overzichtelijke releases beschikbaar te stellen aan de organisatie.

De Opdrachtnemer zal als supplier actief deelnemen in de projectorganisatie. Van de Opdrachtnemer wordt naast de inbreng in de feitelijke beschikbaar stellen en Inrichten van de ITSM-oplossing, verwacht dat zij de Belastingdienst adviseert over inrichtingskeuzes, aanpak en volgorde van Inrichting.

Na de definitieve gunning van de opdracht zal een kick-off met de Opdrachtnemer worden georganiseerd waar de verdere samenwerking en besturing vorm gegeven worden en gezamenlijk de inhoudelijke aanviagroute worden bepaald.

1.2.2. Inzet van de practices

Van de practices die, conform paragraaf 2.5 en paragraaf 2.5.1 van het Beschrijvend document [versie 1.2](#) in scope van de opdracht zijn, zijn er een aantal die, indien deze worden verworven, functioneel volledig worden ingezet. Er zijn ook een aantal practices die bij afname enkel en alleen ingezet worden met als doel te integreren met bestaande en/of toekomstige applicaties (die niet vervangen worden). Met behulp van die practices worden in dat geval naadloze en betrouwbare koppelingen tussen de ITSM-oplossing en de betreffende applicaties gerealiseerd.

Een voorbeeld hiervan is Flexera. (Op dit moment wordt Flexera ingezet als Software Asset Management oplossing omdat deze door grote softwareleveranciers wordt geaccepteerd om licentiebeheer uit te voeren.) De practice IT Asset Management (Software Asset Management Integratie) dient in dit specifieke voorbeeld als integratiestuk tussen Flexera en de ITSM-oplossing.

In de onderstaande tabel is aangegeven van welke practices de functionaliteit bij afname volledig worden geïmplementeerd en welke alleen voor integratie worden gebruikt:

Practice	Doel	Practice	Doel
Change Enablement	Volledig	Availability Management	Integratie
Deployment Management	Volledig	Capacity & Performance Management	Integratie
Incident Management	Volledig	Information Security Management	Integratie
IT Asset Management	Volledig	Risk Management	Integratie
Knowledge Management	Volledig	Monitoring and Event Management	Integratie
Measurement and reporting	Volledig	Supplier Management	Integratie
Problem Management	Volledig		
Release Management	Volledig		
Service Catalog Management	Volledig		
Service Configuration Management	Volledig		
Service Desk	Volledig		
Service Financial Management	Volledig		
Service Level Management	Volledig		
Service Request Management	Volledig		

Tabel 1 overzicht op alfabetische volgorde van practices t.b.v. volledige inzet of Integratie

1.3. Offerteproces

Voor het lichten van Herzieningsclausules zoals beschreven in paragraaf 2.5.1. van het Beschrijvend document [versie 1.2](#), Uitbreidingen, Additionele Diensten in de vorm van consultancy en/of Opleidingen wordt een Offertetraject gestart als Prijzen en/of Tarieven niet vaststaan.

De werkwijze van een Offertetraject is in grote lijnen als volgt:

1. Het IUC Belastingdienst stuurt een aanvraag naar de Opdrachtnemer;
2. De Opdrachtnemer stuurt de Offerte, inclusief met de originele door de Fabrikant en/of toeleverancier afgegeven Offerte retour aan het IUC Belastingdienst;
3. Na goedkeuring van de Opdrachtgever op de Offerte accepteert het IUC Belastingdienst de Offerte door middel van een addendum op de Overeenkomst en een Inkoopopdracht.

De Aanbestedende dienst kan in een Offertetraject de Fabrikant en/of toeleverancier dezelfde Wensen voorleggen als die nu in deze aanbesteding aan de Inschrijver worden gevraagd.

Van de Offerte moet de oorsprong vast te stellen te zijn en te herleiden naar de Fabrikant en/of toeleverancier. Hiervan is bijvoorbeeld sprake indien de Offerte op briefpapier van de Fabrikant wordt aangeleverd. Offertes in pdf van de Fabrikant of doorgestuurde e-mails van de Fabrikant behoren ook tot de mogelijkheden zolang de oorsprong vastgesteld kan worden.

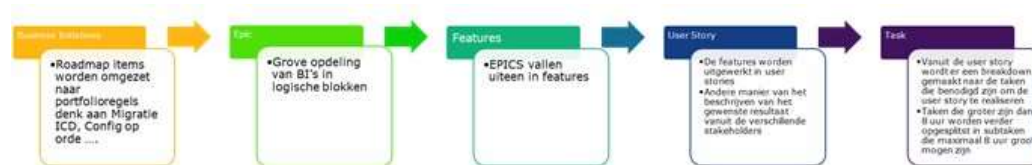
UE 1.	Opdrachtnemer conformeert zich aan de werkwijze van een Offertetraject zoals beschreven in paragraaf 1.3.
UE 2.	Opdrachtnemer hanteert voor elke Offerte een geldigheidstermijn van minimaal 60 dagen.
UE 3.	Opdrachtnemer levert Offertes alléén via het Inkoopuitvoeringscentrum Belastingdienst aan.

1.4. Samenwerken conform Agile/ aanpak, Inrichting en Migratie

De initiële Inrichting, Migratie en de doorontwikkeling van de door u aangeboden ITSM-oplossing, wordt op een Agile wijze ingericht. Hierbij wordt zoveel mogelijk aangesloten bij SAFe (de standaard binnen de Belastingdienst voor Agile werken).

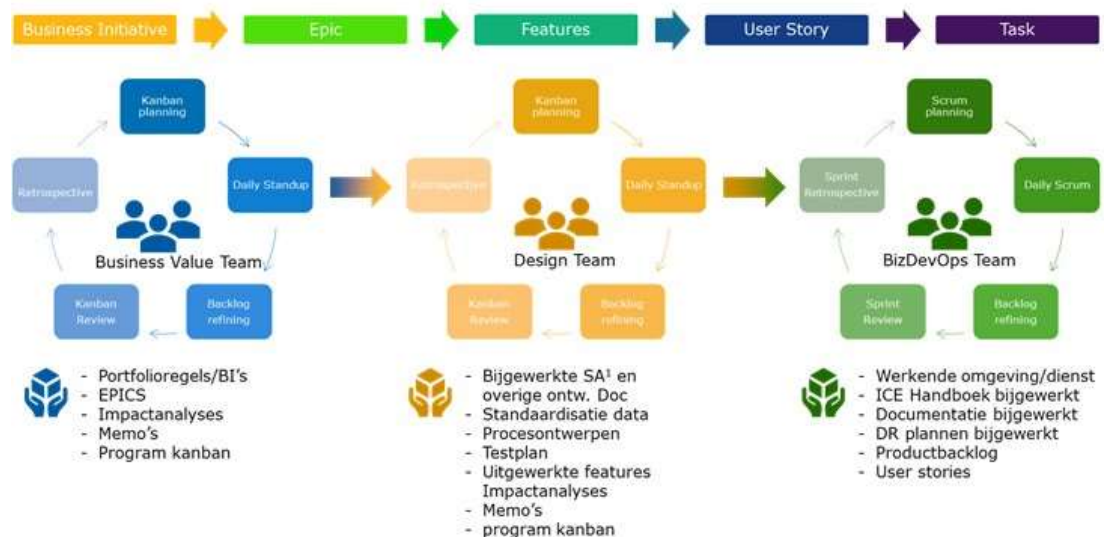
De verwachting is dat voor de Inrichting, Migratie en doorontwikkeling kan worden volstaan met de “essential” inrichting van SAFe.

De methode van werken voor de Inrichting van de nieuwe aan te schaffen ITSM-oplossing is hieronder weergegeven, als mede de teams en de functies die daarvoor ingevuld dienen te worden.



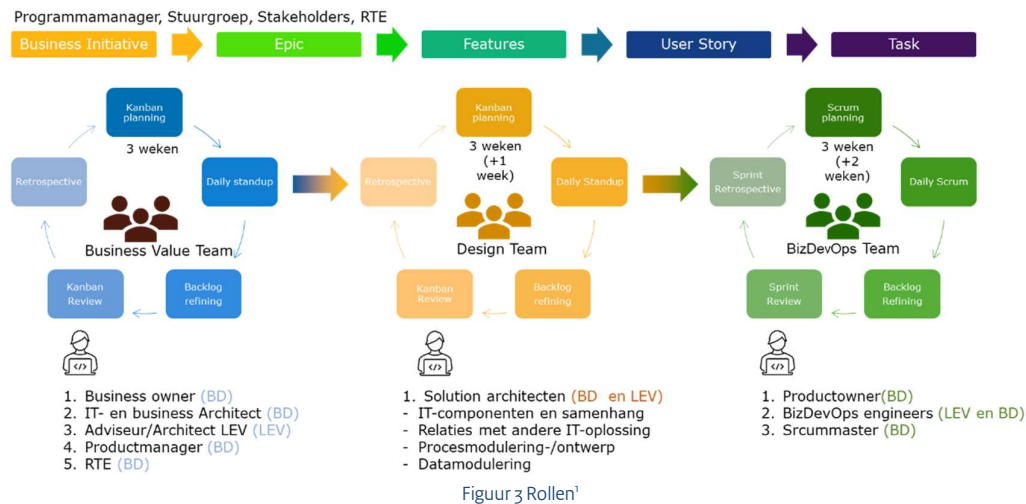
Figuur 1 Werkverdeling

Daarbij worden de volgende teams geformeerd:



Figuur 2 Samenstelling teams

Binnen deze teams zijn de volgende rollen onderkend:



Voor een succesvolle Inrichting moet er achter de business owner nog een organisatie worden ingericht om de met de Inrichting noodzakelijk business change succesvol te implementeren. Dit zal worden opgepakt vanuit een project dat wordt opgezet bij de Belastingdienst. De rollen die hiervoor nodig zijn (denk aan programma-/projectmanagement, verandermanagement, procesmanagement en diepgaander kennis van ITIL4/IT4IT aan business zijde, functioneel beheer aan business zijde) worden door de Belastingdienst zelf ingevuld en indien nodig vindt inhuur plaats de inhuurmantels die de Belastingdienst heeft. Deze rollen zijn dus geen onderdeel van deze aanbesteding.

Van de Opdrachtnemer wordt verwacht dat hij volgende rollen in het project invult:

- Voor het business value team een Adviseur-/Architect;
- Voor het designteam de rol van solution architect vanuit de Opdrachtnemer;
- Voor het BizDevOps team BizDevOps engineers die de ITSM-oplossing configureren.

Er wordt met bovenstaande opzet van teams begonnen. Gaande het proces van Inrichten, migreren en optimaliseren zal deze opzet verder geëvalueerd worden met de betrokken medewerkers en, indien nodig, worden aangepast.

Na contractering wordt begonnen met Business Value team en het Designteam. Het BizDevOps team start pas nadat de ITSM-oplossing technisch in de OTA(P) is ingericht. De engineers kunnen immers pas starten met Inrichten als de ITSM-oplossing technisch ingericht is.

Zie voor de dimensionering van de inzet Bijlage VIII Prijzenformulier versie 1.1, tabblad 3 Additionele Diensten.

De beschrijvingen waaraan elke rol moet voldoen is beschreven in Bijlage 6 Rolbeschrijvingen, versie 1.1.

UE 4. Opdrachtnemer conformeert zich aan de werkwijze zoals beschreven in paragraaf 1.4.

¹ BD betreft medewerkers van de Belastingdienst; LEV betreft medewerkers van/via de Opdrachtnemer.

Hoofdstuk 2. Functionals

2.1. Algemeen

GUE 1.	De ITSM-oplossing biedt de mogelijkheid voor verschillende (interne) klanten van de Opdrachtgever een logisch gescheiden omgeving in te richten.
GUE 2.	In aanvulling op GUE 1 is het in de ITSM-oplossing mogelijk om voor verschillende (interne) klanten, Gegevens tussen de verschillende logisch gescheiden omgevingen uit te wisselen.
GUE 3.	De user interface van de ITSM-oplossing voldoet aan geldende WCAG AA richtlijnen. Zie voor meer informatie: https://www.digitaleoverheid.nl/toegankelijkheidsverklaring/
GUE 4.	De ITSM-oplossing bevat een voor iedere gebruiker toegankelijke Knowledge database.
GUE 5.	De Knowledge database beschikt over een zoekfunctie.
GUE 6.	Inschrijver toont op verzoek aan dat de ITSM-oplossing een aantoonbaar level 4-implementatie van IT4IT (zie https://pubs.opengroup.org/it4it/refarch20/chap04.html) heeft voor de ITSM-oplossing zoals beschreven in paragraaf 2.5 en paragraaf 2.5.1. van het Beschrijvend document versie 1.1.
GUE 7.	Alle Gegevens in de ITSM-oplossing zijn en blijven eigendom van de Aanbestedende dienst.

2.2. Archiveren

GUE 8.	De ITSM-oplossing biedt de mogelijkheid om Gegevens die niet meer actueel zijn (denk hierbij aan bijvoorbeeld aan afgestoten CI's Assets, gesloten Incidenten, Changes etc.) conform de Archiefwet te archiveren en/of te verwijderen . Zie voor meer informatie de Archiefwet .
--------	---

2.3. Rapportage

GUE 9.	De ITSM-oplossing beschikt over een rapportage framework.
GUE 10.	Het rapportage framework bevat standaard sjablonen voor/bij alle practices.
GUE 11.	Over alle Gegevens in de ITSM-oplossing moet gerapporteerd kunnen worden.

W 1	Beschrijf in maximaal 4 pagina's welke mogelijkheden het rapportageframework biedt: De beoordelingscriteria voor deze Wens zijn: - Welke rapportage is standaard in de ITSM-oplossing aanwezig; - Kan elke gebruiker zijn/haar eigen rapportage samenstellen? - Kan elke gebruiker in de eigen rapportage teksten toevoegen? - Kunnen rapportage instellingen gedeeld worden? - Kunnen rapportages per tijdseenheid automatisch samengesteld en gemaild worden? - Kunnen rapportages op onderwerp en/of organisatieonderdeel worden gegenereerd? - Hoe flexibel is het framework bij bijvoorbeeld aanpassingen in de organisatie? - Kan elke gebruiker d.m.v. slepen van velden de rapportage zelf, zonder programmeercodering samenstellen? - Welke presentatie mogelijkheden (bijvoorbeeld, maar niet limitatief, xls, xlsx), html en/of pdf biedt de rapportage tool t.b.v. publicatie van rapportages op het intranet van de Belastingdienst? Voor deze Wens geldt de volgende waardering: <table> <tr> <td>0</td><td>Zeer slecht;</td></tr> <tr> <td>28</td><td>Slecht;</td></tr> <tr> <td>143</td><td>Matig;</td></tr> <tr> <td>236</td><td>Voldoende;</td></tr> <tr> <td>616</td><td>Goed;</td></tr> <tr> <td>945</td><td>Uitstekend.</td></tr> </table>	0	Zeer slecht;	28	Slecht;	143	Matig;	236	Voldoende;	616	Goed;	945	Uitstekend.
0	Zeer slecht;												
28	Slecht;												
143	Matig;												
236	Voldoende;												
616	Goed;												
945	Uitstekend.												

2.4.

Selfservice

ITSM Selfservice portal

Een Selfservice portal is een moderne gebruikersinterface die vanaf elk apparaat vanaf elke locatie toegankelijk is en een onderdeel van de ITSM-oplossing.

Medewerkers bezoeken de Selfservice portal om bijvoorbeeld een oplossing voor hun problemen en/of vragen te vinden. De Selfservice portal maakt het vinden van oplossingen op vragen eenvoudig door directe toegang tot een Knowledge database. Maar ook voor het maken van meldingen (b.v. bestellingen, Incidenten, etc.) en het monitoren van de voortgang op de meldingen

GUE 12.	De ITSM-oplossing beschikt over een Selfservice portal.
GUE 13.	Vanuit de Selfservice portal is toegang tot de Knowledge database.
GUE 14.	De Selfservice portal beschikt over een Chat(ro)bot functie.
GUE 15.	De Chat(ro)bots met virtuele assistenten kunnen dienen als proxy tussen een gebruiker en de Servicedesk.
GUE 16.	De ITSM-oplossing biedt de mogelijkheid de service catalog (logisch) te rubriceren.
GUE 17.	Een Eindgebruiker ziet alleen items van de service catalog waartoe hij/zij rechten heeft.
GUE 18.	De ITSM-oplossing biedt de mogelijkheid om vanuit de Selfservice portal een melding naar de (interne) Helpdesk te sturen.
GUE 19.	De ITSM-oplossing biedt de mogelijkheid om vanuit de selfservice Request Full Fillment bestellingen te plaatsen en volgen.

GUE 20. De ITSM-oplossing biedt de mogelijkheid de status van meldingen en/of bestellingen op te vragen.

2.5. Proces inrichting

GUE 21. De ITSM-oplossing bevat voor-gedefinieerde sjablonen, blueprints en workflows van de ITIL practices die kunnen worden aangepast.

2.6. Technische interface integratie

GUE 22. De ITSM-oplossing ondersteunt voor alle practises van de ITSM-oplossing een functionele ontsluiting via een REST-API.

GUE 23. Inschrijver heeft een beschrijving van de REST-API interface beschikbaar.

GUE 24. De ITSM-oplossing ondersteunt een interface die in staat is minimaal 100.000 items per uur te importeren en/of updaten.

GUE 25. De ITSM-oplossing ondersteunt bulkimport van in ieder geval .csv, .xls en fixed lenght.

In de huidige situatie zijn een groot aantal systemen met ICD gekoppeld. Deze koppelingen zijn ook in de ITSM-oplossing noodzakelijk. Het heeft de voorkeur dat de Inschrijver over standaard koppelingen beschikt om deze systemen te koppelen.

W 2	Geef aan of uw ITSM-oplossing standaard koppelingen heeft met:	
	Flexera Flexnet Manager	95 punten;
	SAP t.n.v. HR, Artikelen, exemplaren van artikelen en Contracten	14 punten;
	Atlassian JIRA	48 punten;
	Atlassian Confluence	48 punten;
	VMWare Workspace One	48 punten;
	Azure DevOps	48 punten;
	Fortes Change Cloud	14 punten.
Op deze Wens kunnen maximaal 315 punten worden behaald.		

GUE 26. De ITSM-oplossing bevat een interface naar SMTP en IMAP.

2.7. Koppelingen

Een oplossing staat zelden op zichzelf. Ook niet als het in de Cloud staat. Oplossingen zijn vaak met andere ICT-systemen binnen de Belastingdienst gekoppeld. Denk ook aan de kantooromgeving van de Belastingdienst. Of aan gebruikers van buiten de Belastingdienst die de Belastingdienst toegang wil verlenen tot, in dit geval, de ITSM-oplossing.

Medewerkers van de Aanbestedende dienst werken met een standaard werkplek. Alleen goedgekeurde Programmatuur kan vanuit een centraal punt geïnstalleerd worden. In de praktijk komt het erop neer dat naast een (standaard) webbrowser geen gebruik gemaakt kan worden van additionele Programmatuur (zoals browser plug-ins) of additionele Apparatuur (zoals dongles). Dit noemt de Aanbestedende dienst een zero-footprint client.

In de praktijk betekent dat dat er gebruik wordt gemaakt van een web browser als clientprogramma. De Aanbestedende dienst ondersteunt op de eigen werkplek Google Chrome.

GUE 27.	De ITSM-oplossing ondersteunt de laatste twee (2) versies van de ondersteunde webbrowsers, zonder gebruik te maken van aanvullende Programmatuur. Zie voor meer informatie: https://www.communicatierijk.nl/vakkennis/rijkswebsites/aanbevolen-richtlijnen/browsersupport .
---------	--

Gegevens worden niet alleen binnen de ITSM-oplossing verwerkt. Er zal ook sprake zijn van transport van Gegevens van en naar de ITSM-oplossing en mogelijk tussen de verschillende onderdelen binnen de ITSM-oplossing, of zelfs derde partijen. Ook als de ITSM-oplossing uit meerdere deeloplossingen bestaan die niet direct met elkaar gekoppeld zijn, maar bijvoorbeeld via het internet, dan is er sprake van transport van Gegevens (Gegevens in transitie).

Gegevens in transitie worden versleuteld. Versleuteling is gebaseerd volgens de richtlijnen van het NCSC. In Bijlage 9 ICT-beveiligingsrichtlijnen-voor-Transport-Layer-Security-v2 zijn in hoofdstuk 4 richtlijnen en voorwaarden beschreven. Op de website van het NCSC is altijd de meest recente richtlijn te vinden. Voor de ITSM-oplossing geldt dat deze aan elke richtlijn moet voldoen aan het criterium 'Goed'.

Zie ook: <https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1>

GUE 28.	De ITSM-oplossing voldoet aan elke in genoemde in hoofdstuk 4 (Versies, algoritmes en opties) van Bijlage 9 ICT-beveiligingsrichtlijnen-voor-Transport-Layer-Security-v2 genoemde TLS-versies, Cryptografische algoritmes, sleutellengtes en keuze van groepen en overige opties die met een 'Goed' worden gewaardeerd.
---------	---

UE 5.	In navolging van GUE 28 zorgt Opdrachtnemer dat de ITSM-oplossing meegroeit in de richtlijnen en de implementatie ervan. Afspraken hier omtrent worden vastgelegd in een DAP met de Belastingdienst.
-------	--

UE 6.	Opdrachtnemer is verantwoordelijk dat koppelingen tussen de ITSM-oplossing en systemen van derden beveiligd zijn.
-------	---

2.8.

Forum Standaardisatie

De Belastingdienst is als overheidspartij gehouden aan de standaarden, zoals vastgesteld door het Forum Standaardisatie. De verplichte standaarden worden toegepast conform het Pas-toe-of-leg-uit-principe (Comply-or-Explain). Van een aantal standaarden heeft de Belastingdienst overigens vastgesteld dat Inschrijver deze moet toepassen (dus zonder Leg-uit-mogelijkheid).

Zie ook: <https://www.forumstandaardisatie.nl/open-standaarden/verplicht>

Dit is ook van toepassing gedurende de looptijd van de Overeenkomst. Als deze lijst met standaarden of de standaarden zelf inhoudelijk wijzigen zullen tussentijds afspraken gemaakt worden.

Voor de ITSM-oplossing zijn onderstaande standaarden verplicht:

GUE 29.	De ITSM-oplossing biedt de mogelijkheid om voor alle webverbindingen van de ITSM-oplossing HTTPS en HSTS toe te passen conform de richtlijnen van het NCSC. Hierbij geldt dat alleen gebruik gemaakt wordt van standaarden en instellingen die door het NCSC als 'Goed' zijn gekwalificeerd ("ICT-beveiligingsrichtlijnen voor Transport Layer Security") en moet op de 'Qualys SSL Labs SSL Server Test' minimaal een A- worden behaald. Zie https://www.ssllabs.com/ssltest/index.html
---------	---

GUE 30.	De ITSM-oplossing moet transparant zijn voor zowel IPv4 als IPv6.
---------	---

GUE 31.	De ITSM-oplossing biedt de mogelijkheid om voor elke domeinnaam van de ITSM-oplossing, voor communicatie met bedrijven die werkzaamheden voor IV uitvoeren, gebruik te maken van DNSSEC. De
---------	---

	domeininformatie, zoals bijbehorende IP-adressen, is met een geldige DNSSEC-handtekening ondertekend.
--	---

Het is mogelijk dat tijdens de looptijd van de Overeenkomst er wijzigingen optreden in de lijst met Open Standaarden. In een dergelijk geval treden partijen in overleg wat hiermee te doen.

UE 7.	Opdrachtnemer gaat akkoord om in overleg te treden als de lijst Open Standaarden wijzigt.
-------	---

2.9. Eisen aan practices

GUE 32.	Het is mogelijk bij iedere practice van de ITSM-oplossing bijlages met minimaal de extensies pdf, zip, txt, doc, docx, dwg, gif, csv, xls, xlsx, ppt, xml, xsl, bmp, html, png, pptx, cfr, jpeg, mp4, mov, odt, ods, odp, jpg, jpeg, rtf, wmv, wm, wma en xlsx toe te voegen.
---------	---

GUE 33.	Elke practice binnen de ITSM-oplossing heeft de mogelijkheid voor opmaak van tekst; dit betekent het aan kunnen passen van bijvoorbeeld lettertype, lettergrootte, opsommingstekens etc.
---------	--

GUE 34.	De ITSM-oplossing toont de status van de voortgang binnen een proces van de betreffende geïmplementeerde practice.
---------	--

Hoofdstuk 3. IV kaders

Vanuit IV zijn de navolgende Eisen en Wensen gedefinieerd.

3.1. Non-functionals

Gebruikersinterface

GUE 35.	Behandelaars zijn in staat, na het lezen van gebruikersinstructies en/of een opleiding van maximaal 1 dag, zelfstandig te werken met de ITSM-oplossing.				
GUE 36.	De user interface van de ITSM-oplossing is minimaal beschikbaar in de Nederlandse en Engelse taal.				
GUE 37.	De gebruiker heeft de mogelijkheid om m.b.t. de user interface binnen de ITSM-oplossing zelf de keuze te maken voor de Nederlandse en/of Engelse taal.				
GUE 38.	De ITSM-oplossing ondersteunt het Inrichten van het startscherm op basis van rollen.				
GUE 39.	De ITSM-oplossing ondersteunt voor elke gebruiker de mogelijkheid om een eigen startscherm in te richten/ in te stellen.				
W 3	Geef aan of de ITSM-oplossing de Nederlandse en Engelse taal ten aanzien Natural Language Query ondersteunt. De beoordelingscriteria voor deze Wens zijn: <table> <tr> <td>Beide talen worden ondersteund</td><td>810 punten;</td></tr> <tr> <td>Alleen Nederlands, alleen Engels of geen van beide</td><td>0 punten.</td></tr> </table>	Beide talen worden ondersteund	810 punten;	Alleen Nederlands, alleen Engels of geen van beide	0 punten.
Beide talen worden ondersteund	810 punten;				
Alleen Nederlands, alleen Engels of geen van beide	0 punten.				
GUE 40.	De web interface m.b.t de ITSM-oplossing voldoet aan Responsive Web design; dit houdt in dat de interface zich aanpast aan het Device waarop het wordt aangeroepen.				

Performance

GUE 41.	Bij het aanmaken van een nieuw Incident in de ITSM-oplossing is het betreffende scherm binnen maximaal 5 seconden beschikbaar om Gegevens in te voeren.
---------	---

Autorisaties

GUE 42.	De ITSM-oplossing ondersteunt een RBAC model voor zowel data als functionaliteit.
GUE 43.	De ITSM-oplossing kent verschillende autorisatieniveaus.
GUE 44.	Een gebruiker mag in zijn/haar GUI geen opties zien waarvoor die niet is geautoriseerd.

Subscriptions

GUE 45.	De ITSM-oplossing geeft inzicht in het gebruik van Subscriptions van de ITSM-oplossing.
---------	---

GUE 46.	De ITSM-oplossing informeert Opdrachtgever wanneer het aantal aangeschafte Subscriptions door gebruik overschreden wordt. Dit kan bijvoorbeeld door een (automatisch) alert in de vorm van een e-mail aan een in te stellen contactpersoon.
---------	---

Generieke aansluitvoorwaarden

GUE 47.	De ITSM-oplossing voldoet aan Bijlage 7 IDWOR (interoperabiliteitskader voor digitale werkomgevingen in de rijksdienst)
---------	---

3.2. Beveiliging

3.2.1. Privacy

GUE 48.	De naleving van de AVG door de Belastingdienst wordt niet door de ITSM-oplossing gehinderd.
GUE 49.	In aanvulling tot GUE 48 geldt dat de ITSM-oplossing conform privacy by design is gebouwd.
GUE 50.	In aanvulling tot GUE 48 geldt dat de ITSM-oplossing conform privacy by default is gebouwd.
GUE 51.	De ITSM-oplossing biedt de mogelijkheid om persoonsgegevens af te schermen.
GUE 52.	De ITSM-oplossing biedt de mogelijkheid om Gegevens versleuteld op te slaan zodat de informatie niet toegankelijk is voor medewerkers van Opdrachtnemer.
UE 8.	Opdrachtnemer deelt en/of gebruikt geen Gegevens voor eigen doeleinden, anders dan strikt noodzakelijk voor de uitvoering van de Overeenkomst én dan alleen ná expliciete toestemming van de Opdrachtgever. In geval toont Opdrachtnemer aan welke Gegevens om welke reden(en) strikt noodzakelijk zijn.
UE 9.	Opdrachtnemer zal, in navolging van UE 8, aangeven welke Gegevens in een dergelijk geval als noodzakelijk worden geacht voor de uitvoering van de Overeenkomst.

Gegevens die te relateren zijn aan de Belastingdienst of haar medewerkers mogen zonder expliciete toestemming van de Opdrachtgever niet buiten de ITSM-oplossing verwerkt worden. Dat geldt uiteraard ook voor Persoonsgegevens. Productiegegevens worden alleen in de Productieomgeving verwerkt. Buiten de Productieomgeving zijn de Gegevens, conform marktstandaarden, bijvoorbeeld die van de NCSC, gepseudonimiseerd of geanonimiseerd. Opdrachtnemer geeft de Opdrachtgever vooraf inzicht in hoe dit plaats vindt.

UE 10.	Opdrachtnemer conformeert zich, conform bovenstaande alinea, aan dat bij testen van de ITSM-oplossing geen gebruik wordt gemaakt van: - Productiegegevens; - Naar natuurlijke personen herleidbare Gegevens. Indien het voor het testen van de ITSM-oplossing noodzakelijk is om Productiegegevens te gebruiken of Gegevens die herleidbaar zijn naar natuurlijk personen, dan moeten beveiligingsmaatregelen, gelijk aan die van de Productie-omgeving, getroffen worden en moet er een door de Opdrachtgever ondertekende Waiver overlegd worden. Deze Waiverprocedure wordt vastgelegd in een DAP met de Belastingdienst.
--------	---

Beschikbaarheid, integriteit en vertrouwelijkheid van Gegevens van de Belastingdienst mogen op geen enkele manier gecompromitteerd raken. Van medewerkers van Opdrachtnemer met toegang tot Gegevens en ITSM-oplossing wordt vooraf de achtergrond gecontroleerd. Voor Nederlandse ingezetenen wordt gebruik gemaakt van de VOG (algemeen screeningsprofiel, functie-aspecten: 11, 12, 13 en 41). Voor niet ingezetenen kan een gelijkwaardige verklaring worden overlegd. De Opdrachtgever oordeelt over de bruikbaarheid hiervan.

Niet Nederlandse ingezetenen kunnen voor informatie terecht bij Justis. Zie voor meer informatie:

<https://www.justis.nl/service-contact/veelgestelde-vragen/vog/hoe-kan-ik-een-vog-aanvragen-als-ik-niet-ben-ingeschreven-in-de-brp#:~:text=Sluiten-.Hoe%20kan%20ik%20een%20VOG%20aanvragen%20als%20ik%20niet%20ben.VOG%20rechtstreeks%20bij%20Justis%20aanvragen>

en

<https://www.rijksoverheid.nl/wetten-en-regelingen/productbeschrijvingen/aanvragen-verklaring-omtrent-het-gedrag-vog-bij-justis>

UE 11.	Opdrachtnemer beschikt voor medewerker(s) die werkzaamheden m.b.t. genoemde Gegevens gaan uitvoeren, over een geldige Verklaring Omtrent Gedrag (hierna VOG.)
--------	---

3.2.2. Gegevens

De Gegevens van de Belastingdienst moeten gescheiden worden verwerkt (waaronder opgeslagen) van andere klanten van Opdrachtnemer; de Belastingdienst wil geen zicht hebben in Gegevens van andere klanten van de Opdrachtnemer en andere klanten mogen geen zicht in de Gegevens van de Belastingdienst hebben. Medewerkers van Opdrachtnemer mogen alleen toegang hebben tot de Gegevens van de Belastingdienst voor zover dat noodzakelijk is voor het uitvoeren van de Overeenkomst.

GUE 53.	Gegevens van de Belastingdienst worden gescheiden opgeslagen van de Gegevens van andere klanten van de Inschrijver.
---------	---

GUE 54.	Toegang tot Gegevens van de Belastingdienst is beperkt voor medewerkers van de Belastingdienst en medewerkers van de Inschrijver voor zover dit noodzakelijk is voor de uitvoering van de Overeenkomst.
---------	---

De Aanbestedende dienst maakt bij voorkeur gebruik van versleutelde Gegevens bij opslag. Eén van de voordelen is dat als de Gegevens op ongecontroleerde wijze buiten de ITSM-oplossing terecht komen, andere partijen geen gebruik kunnen maken van deze Gegevens.

GUE 55.	Data in de ITSM-oplossing is versleuteld. Encryption-at-rest en encryption-in-transit is hierbij toegepast.
---------	---

GUE 56.	Met betrekking tot GUE 55 geldt dat de private key zowel bij de Opdrachtgever dienst als de Opdrachtnemer in beheer moet kunnen worden gegeven.
---------	---

Met de doorontwikkeling van quantumtechnologie ontstaat een nieuw type computersystemen dat ongekende mogelijkheden geeft. Naast veelbelovende kansen dient zich de dreiging aan dat cryptografische versleutelingen niet meer veilig zullen zijn. Daarbij komt dat met het zogeheten 'steal now, decrypt later'-scenario ook vandaag al sprake is van dreiging. De Aanbestedende dienst vindt het belangrijk om te bewegen richting 'crypto agility' en de implementatie van quantum veilige cryptografie. 'Crypto agility' betekent dat een organisatie gemakkelijk geïmplementeerde cryptografische primitieven kan aanpassen of vervangen zonder dat dit tot bovenmatige verstoringen leidt. Voor meer informatie, zie: <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/quantumveilige-cryptografie>.

Hieruit is de onderstaande Wens ontstaan:

W 4	Beschrijf op welke wijze u voorbereidingen treft om de risico's en dreiging die uit gaan van quantumtechnologie te mitigeren en wat de impact daarvan is op de ITSM-oplossing. De beschrijving bevat minimaal de volgende onderwerpen: - Op welke wijze u inzicht heeft in: - De cryptografische componenten die deel uitmaken van (de systemen die deel uitmaken van) de ITSM-oplossing; - De use cases waarvoor deze cryptografische componenten worden ingezet ('in use', 'in transit', 'at rest'); - De mate waarin deze componenten kwetsbaar zijn voor aanvallen met quantum computers. - De aanwezigheid van een migratieplan voor de migratie naar quantum veilige cryptografie en zo ja, wat de status daarvan is; - Welke verschillende stappen en mijlpalen u ziet in het migratieproces die de ITSM-oplossing raken.
-----	---

4. De wijze waarop u 'crypto agility', of stappen in die richting, realiseert in de ITSM-oplossing.
5. Op welke wijze uw organisatie samen met de Opdrachtgever kan verifiëren dat Releases en aanpassingen leiden tot correcte werking en inzetbaarheid van de ITSM-oplossing. Achtergrond is dat het voor sommige cryptografische implementaties van belang is dat beide partijen eenzelfde of complementaire implementatie hebben toegepast voor een correcte werking.
6. Een beschrijving hoe knelpunten worden verholpen.

De beschrijving is, exclusief voorblad, inhoudsopgave en afbeeldingen, maximaal 3 pagina's. Hyperlinks en/of verwijzingen naar andere documenten en/of websites zijn niet toegestaan.

De beoordelingscriteria voor deze Wens zijn:

- De mate waarin uw beantwoording inzicht geeft in hoe uw organisatie gestructureerd toe werkt naar implementatie van 'crypto agility' en quantum veilige cryptografie in de ITSM-oplossing (en de systemen die daarvan deel uitmaken). Openheid over concrete maatregelen en stappen, zowel organisatorisch als technisch, geeft daarbij een beter beeld dan algemene termen;
- De manier waarop uw beantwoording uitwerking geeft aan gezamenlijke verantwoordelijkheid van uw organisatie en de Belastingdienst rondom de inzet van quantum veilige cryptografie.

Voor deze Wens geldt de volgende waardering:

0	Zeer slecht;
24	Slecht;
122	Matig;
201	Voldoende;
527	Goed;
810	Uitstekend.

3.2.3. Beveiligingsincidenten

Dit zijn Incidenten die een vermoedelijk of mogelijk opzettelijke inbreuk veroorzaken op de beschikbaarheid, vertrouwelijkheid of integriteit van de Gegevens in informatie verwerkende systemen of inbreuk maken op deze systemen zelf.

Voor beveiligingsincidenten geldt dat bij ontdekking/melding zowel de Impact als Urgentie als Hoog worden gekwalificeerd wat resulteert in een prioriteit 1 Incident. Een beveiligingsincident wordt altijd per direct opgevolgd met een actie van de Opdrachtnemer.

Na een eerste evaluatie kan onderbouwd besloten worden de prioriteit te verlagen. De Opdrachtgever heeft hierbij het laatste woord.

Er worden vier typen beveiligingsincident onderkend:

1. (Cyber)hack, of een poging daartoe;
2. Coordinated Vulnerability Disclosure (CVD, voorheen Responsible disclosure);
3. Kwetsbaarheid via CVE-database of Security Note van leverancier van ICT-component of beveiligingsberichten van CERTs (NCSC, bedrijfstak- of sectorgerichte CERT) en
4. Kwetsbaarheid vanuit beveiligingstest (A&P-test of Vulnerability scan)

Als waarderingsmethodiek voor Kwetsbaarheden wordt gebruik gemaakt van de meest recente versie van marktstandaard Common Vulnerability Score System (CVSS, momenteel versie 3.1). Oplostermijnen die hier aan gekoppeld zijn, zijn:

- Kritisch risico (Critical risk, score 9.0 – 10.0): per direct (voor lifegang van een nieuwe oplossing is dit belemmerend). Voor de Opdrachtgever is dit een incident;
- Hoog risico (High risk, score 7.0 – 8.9): per direct, na afstemming maximaal 1 maand (voor lifegang van een nieuwe oplossing is dit belemmerend). Voor de Opdrachtgever is dit een incident;
- Gemiddeld risico (Medium risk, score 4.0 – 6.9): 3 maanden. Voor de Opdrachtgever is dit een problem en
- Laag risico (Low risk, 0.1 – 3.9): 6 maanden. Voor de Opdrachtgever is dit een problem.

Voordat de ITSM-oplossing in productie kan gaan, wordt de beveiliging van de ITSM-oplossing getest ter Acceptatie. Daarna gebeurt dat periodiek (minimaal jaarlijks).

Gemiddeld- en Laagrisico bevindingen worden afgehandeld conform het Pas-toe-of-Leg-uitprincipe. Dit laatste, een Leg uit (Explain), betekent dat er besloten is dat de Kwetsbaarheid niet weggenomen wordt of dat adresseren ervan meer tijd gaat kosten dan de standaard Oplostijd. Opdrachtnemer onderbouwt in een dergelijk geval haar besluit (bijvoorbeeld: er zijn afdoende mitigerende maatregelen getroffen waardoor de Kwetsbaarheid niet uitgevoerd hoeft te worden of dat de impact nihil is). Het is aan de Opdrachtgever om akkoord te gaan met een Leg-uit.

Opdrachtgever heeft geen oplossingen in productie staan waarin zich Kwetsbaarheden bevinden die als Kritisch of Hoog risico zijn gekwalificeerd. Bij Kritische- en Hoge risico's kan een Leg-uit alleen gebruikt worden om de oplostermijn (beperkt) op te rekken. Dit kan alleen met nadrukkelijke instemming van de Opdrachtgever.

Het Stekkermanndaat (zie ook paragraaf 3.2.6 **Stekkermanndaat**) wordt in gang gezet als een ICT-oplossing reeds in productie staat. Staat een ICT-oplossing nog niet in productie, dan zal dat ook niet mogen totdat de Kritische-en Hoge risicobevindingen zijn weggenomen.

UE 12.	Uit bovenstaande volgt daarom de Eis dat Opdrachtnemer zich conformeert, gedurende de looptijd van de Overeenkomst, aan de door de Opdrachtgever gebruikte methode (CVSS) om beveiligingsincidenten te kwalificeren en heeft haar organisatie zodanig ingericht dat de door de Opdrachtgever onderkende typen Beveiligingsincidenten voor (onderdelen) van de ITSM-oplossing binnen gestelde termijnen, als onderdeel van het Onderhoud & Support, opgepakt en opgelost worden.
UE 13.	Bij het constateren van Kwetsbaarheden met een niveau van kritisch (critical) of hoog (high), conform CVSS (de huidige bij de Opdrachtgever toegepaste versie CVSS 3.1), wordt de Opdrachtgever daarover binnen één (1) uur door Opdrachtnemer geïnformeerd. Afspraken over het toepassen van een volgende versie van CVSS hier omtrent worden vastgelegd in een DAP met de Belastingdienst.
UE 14.	Kwetsbaarheden die leiden tot een Incident worden gekwalificeerd door middel van CVSS 3.1. Op basis van de CVSS 3.1 kwalificaties gelden voor de Opdrachtnemer de volgende streeftijden om deze op te lossen: • Kritisch (critical): per direct (binnen vier (4) uren) op te lossen; • Hoog (high): binnen één (1) maand; • Gemiddeld (medium): binnen drie (3) maanden; • Laag (low): binnen zes (6) maanden.
GUE 57.	In de ITSM-oplossing gebruikte Open Source-code en/of libraries van andere toeleveranciers bevatten geen bekende Kwetsbaarheden. Er wordt gebruik gemaakt van de meest recente veilige versies uit betrouwbare bron. Op deze GUE mag alleen met NVT worden geantwoord als in de ITSM-oplossing géén Open Source-code en/of libraries van andere toeleveranciers is/zijn verwerkt.

Opdrachtgever gaat er van uit dat Opdrachtnemer de ITSM-oplossing ook levert of gaat leveren aan derden. Indien in dergelijke instances zich inbreuken op beveiliging en/of privacy voordoen, die zich ook kunnen voordoen in de aan de Opdrachtgever geleverde ITSM-oplossing, dan wordt de Opdrachtgever daarvan onverwijld van op de hoogte gebracht om zo nodig mitigerende maatregelen te kunnen treffen. Opdrachtgever monitort dit actief.

Het gaat niet alleen om opgetreden Incidenten, maar ook om mogelijke toekomstige Incidenten waar Opdrachtnemer van kan uitgaan dat deze in de (nabije) toekomst kunnen optreden. Denk aan een zero-day exploit.

Het gaat de Opdrachtgever om het (technisch) inhoudelijke Incident om deze te kunnen analyseren en, zo nodig, mitigerende maatregelen te treffen. Er worden nadrukkelijk geen bedrijfsgegevens van getroffen partijen gedeeld.

Opdrachtnemer zal in dat geval tevens de omvang van het Incident aangeven, de verwachte consequenties voor de Opdrachtgever, alsmede de reeds getroffen en te treffen maatregelen om de gevolgen te beperken.

UE 15.	Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. inbreuken op beveiliging en/of privacy in de ITSM-oplossing bij derden. Het proces hiervoor moet worden beschreven in een DAP met de Belastingdienst.
--------	---

Indien Opdrachtgever (op basis van een risico-inschatting) het noodzakelijk acht een A&P-test uit te laten voeren dan staat Opdrachtnemer dat toe en werkt daar conform afspraken aan mee. De precieze invulling van de A&P-test is afhankelijk van de situatie. Het kan een A&P-test zijn binnen de keten waar de ITSM-oplossing onderdeel van is of op de ITSM-oplossing zelf.

Het organiseren van deze A&P-test gebeurt door Opdrachtgever; het uitvoeren van de A&P-test zelf is voor rekening van Opdrachtgever.

Eventuele Kwetsbaarheden worden opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan. Opdrachtnemer werkt hier als onderdeel van Onderhoud & Support aan mee.

UE 16.	Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. inbreuken op beveiliging en/of privacy in de ITSM-oplossing bij derden.
--------	---

3.2.4. Datalek

De Belastingdienst handelt als verwerkingsverantwoordelijke conform de wettelijke kaders als primaire partij Data incidenten af. De verwerkingsverantwoordelijke moet de Autoriteit Persoonsgegevens (AP) binnen 72 klokuren op de hoogte stellen van een Datalek en eist van Opdrachtnemer onverwijld, doch uiterlijk binnen 24 klokuren op de hoogte te worden gesteld van een door Opdrachtnemer geconstateerd Datalek. Een (potentieel) Datalek is het gevolg van een beveiligingsincident en moet ook als zodanig worden geregistreerd en afgehandeld. Melding aan AP en afhandeling van het corresponderende beveiligingsincident kan parallel plaatsvinden.

Bij het informeren over een Datalek moet de omvang worden aangegeven alsmede de getroffen en/of te nemen maatregelen om de gevolgen te adresseren. In afstemming wordt bepaald welke partij primair analyse en afhandeling uitvoert. Verwerkingsverantwoordelijke en Opdrachtnemer houden elkaar op de hoogte. **Procedures hier omtrent worden vastgelegd in een DAP met de Belastingdienst.**

UE 17.	Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. het omgaan met van een Datalek in de ITSM-oplossing.
--------	--

3.2.5. Coordinated Vulnerability Disclosure

De Aanbestedende dienst heeft een Coordinated Vulnerability Disclosure-procedure (CVD-procedure). Goedwillende beveiligingsonderzoekers kunnen via een vastgesteld proces kwetsbaarheden, mits er geen wetten worden overtreden, melden. Het CVD-proces is op deze pagina beschreven: <https://www.belastingdienst.nl/security#coordinated-vulnerability-disclosure>.

UE 18.	Opdrachtnemer conformeert zich aan bovengenoemde CVD-procedure m.b.t. het afhandelen van CVD-meldingen. Procedures hier omtrent worden vastgelegd in een DAP met de Belastingdienst.
--------	--

3.2.6. Stekkermandaat

Opdrachtgever kent het principe van het Stekkermandaat. Opdrachtgever kan opdracht geven dat de ITSM-oplossing (inclusief de Gegevens) van de Belastingdienst onbeschikbaar gemaakt wordt voor (minimaal) toegang vanaf het internet. Effectief zal dit betekenen dat:

- Gegevens van de Belastingdienst ontoegankelijk worden gemaakt en/of
- (Relevante delen van) de ITSM-oplossing onbeschikbaar worden gemaakt.

Het Stekkermandaat wordt uitgevoerd op het moment dat de beveiliging van de ITSM-oplossing (inclusief Gegevens) in gevaar is. Dat is het geval als er zich een beveiligingsincident met een score van Kritisch of Hoog risico voordoet waarbij de onderliggende Kwetsbaarheid niet tijdig kan worden weggenomen.

De ITSM-oplossing wordt weer in productie (online) gebracht na toestemming van de Security Officer van de Belastingdienst.

Opdrachtnemer werkt, daar waar relevant, kosteloos mee bij:

- Het onbeschikbaar en ontoegankelijk maken van de ITSM-oplossing of de Gegevens (dit is inclusief andere portalen en koppelingen);
- Exportaties van Gegevens indien het proces via een andere oplossing/procedure voortgezet dient te worden bij Opdrachtgever.

Het proces en de afspraken hiervoor worden beschreven in een DAP met de Belastingdienst.

UE 19.	Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. het omgaan met van het Stekkermandaat in relatie tot de ITSM-oplossing. Hierbij geldt dat tussen het inroepen van het Stekkermandaat en het afronden van de uitvoering maximaal 4 uur zit. Het startmoment begint als het verzoek om Gegevens veilig te stellen door Opdrachtnemer is ontvangen.
--------	--

Bij (langdurige) uitval van de ITSM-oplossing krijgt de Opdrachtgever de beschikking over de meest recente Gegevens. Aanlevering gebeurt via een afgestemd veilig kanaal en conform afspraken conform (machine leesbaar) formaat.

UE 20.	Opdrachtnemer levert op aanvraag en conform afspraken een voor de Belastingdienst bruikbare digitale kopie van de meest actuele Gegevens en haar structuur. Vertrouwelijkheid en integriteit blijven geborgd. De afspraken hierover worden in een DAP met de Belastingdienst vastgelegd.
--------	---

Reinstate

Het weer beschikbaar maken van de ITSM-oplossing (Reinstate) houdt in dat de ITSM-oplossing weer in productie wordt gebracht met gebruikmaking van de meest actuele Gegevens. Dit is inclusief importaties van de Gegevens indien het proces via een andere oplossing/procedure voortgezet is geweest.

Hierbij geldt de speciale aandacht voor de situatie dat Gegevens van vóór het stopzetten van de ITSM-oplossing samengevoegd moeten worden met de Gegevens die in de tussentijd, zijn gegenereerd. Integriteit en Vertrouwelijkheid van de Gegevens blijven te allen tijde geborgd.

Opdrachtnemer werkt met betrekking tot bovenstaande alinea's als onderdeel van het Onderhoud & Support mee met het opnieuw in gebruik nemen van de ITSM-oplossing.

De afspraken hierover worden in een DAP met de Belastingdienst vastgelegd.

UE 21.	Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. de Reinstate van de ITSM-oplossing.
--------	---

3.2.7. Beveiligingstesten

Inleiding

Beveiligingstesten zijn een belangrijk onderdeel in het stelsel van beveiligingseisen-en maatregelen. De Opdrachtgever stelt Eisen aan deze beveiligingstesten. Deze Eisen betreffen de testmethode, waardering van de bevindingen, de testende partij, de rapportage en de afhandeling van de Kwetsbaarheden.

Er worden periodiek of rond een omvangrijke release beveiligingstesten uitgevoerd op een internet-facing ICT-oplossing. Het betreffen zowel Attack & Penetration testen als Vulnerability scans. De partij waar primair de hosting plaatsvindt, is de eerst verantwoordelijke om deze beveiligingstesten uit te voeren. Meestal is dat de Opdrachtnemer.

Beveiligingstesten die (aanvullend) uitgevoerd worden door de Opdrachtgever vervangen niet de beveiligingstesten van de Opdrachtnemer. Beveiligingstesten zijn slechts momentopnamen. Herhaling is dus van belang. Net als het hertesten van geadresseerde bevindingen.

De kosten van uitvoering van dergelijke beveiligingstesten worden gedragen door de partij die de beveiligingstest behoort uit te voeren. De andere partij werkt op verzoek kosteloos mee aan dergelijke testen. Onder het kosteloos meewerken, valt onder andere:

- Het beantwoorden van vragen in de verschillende fasen van voorbereiding en uitvoering van een beveiligingstest;
- Het oplossen van bevindingen die uit de beveiligingstesten volgen. Dit is inclusief eventueel benodigd overleg hierover.

De partij die de A&P-test laat uitvoeren bepaalt zelf welke partij de A&P-test uitvoert en wat de inhoud van de A&P-test is. De Opdrachtgever stelt wel Eisen aan de kwaliteit van zowel de A&P-test, als de rapportage daarover.

Bevindingen volgend uit de beveiligingstesten zullen tussen de Opdrachtgever en Opdrachtnemer worden gedeeld en zo nodig besproken. Hetzelfde geldt voor plannen van aanpak en Verbeterplannen. Om de A&P-test te kunnen beoordelen wordt het volgende tussen de partijen gedeeld:

- De scope van de test (infrastructuur, middleware, tooling en (API-)koppelingen) is beschreven. Het is duidelijk welke delen van de ITSM-oplossing binnen en buiten scope zijn geweest. Het is bekend welke beveiligingsmaatregelen (tijdelijk) uitgeschakeld waren;
- Welke testmethodieken (black-, grey- of crystal boxtesting, wel of niet inclusief broncodereview) zijn gebruikt, en welke normenkaders zijn gebruikt (bijvoorbeeld STRIDE, OWASP Top 10, SANS Top 25, OWASP Mobile Top 10, etc.);
- Hoe getest is; geautomatiseerd, handmatig (worden geautomatiseerd gevonden handmatig geverifieerd?);
- Managementsamenvatting met een definitie van de opdracht, relevante kenmerken van de A&P-test, een conclusie en aanbevelingen;
- Alle gevonden Kwetsbaarheden zijn opgenomen in de rapportage met CVSS-waardering. Aangegeven welke versie van CVSS (vanaf 3.0) is gebruikt. Bij voorkeur met de statusaanduiding, bijvoorbeeld "In behandeling" (met plandatum) of "Opgelost (en hertest)".

In een Verbeterplan wordt het volgende opgenomen:

- Onderwerp/naam van het Verbeterpunt;
- Startdatum;
- Geplande einddatum oplossing;
- Beoogde aanpak (kort);
- Status;
- Lessons learned;
- De Security Roadmap.

Aanvullende uitgangspunten bij A&P-testen die door of namens de Opdrachtgever worden uitgevoerd. Hierbij geldt dat:

- Er getest wordt in de Acceptatieomgeving welke technisch gelijk is aan en voorzien is van dezelfde beveiligingsmaatregelen als de Productie-omgeving; voor noodzakelijke afwijkingen is toestemming van de Opdrachtgever vereist;
- Er wordt géén gebruik gemaakt van Productiegegevens; voor noodzakelijke afwijkingen is toestemming van de Opdrachtgever vereist;
- Er is sprake van een freeze-periode in de omgeving wordt getest; alleen in samenspraak met het A&P-testbedrijf, bijvoorbeeld om een patch uit te voeren om een Kwetsbaarheid weg te nemen, kan hier van worden afgeweken;
- Kwetsbaarheden gekwalificeerd als Kritisch of Hoog risico worden zo mogelijk tijdens de A&P-test opgelost en hertest.

Opdrachtgever voert jaarlijks of na een significante release een A&P-test uit conform de hierboven beschreven richtlijnen van de Belastingdienst. De precieze invulling van de A&P-test is afhankelijk van de situatie.

Eventuele Kwetsbaarheden worden als onderdeel van Onderhoud & Support opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan.

UE 22.	Opdrachtnemer conformeert zich aan bovenstaande, onder het kopje Inleiding genoemde, alinea's m.b.t. Beveiligingstesten in relatie tot de ITSM-oplossing.
--------	--

A&P test vanuit Opdrachtgever

Als de Opdrachtgever het noodzakelijk vindt om de sterkte van de beveiligingsmaatregelen van de ITSM-oplossing te (laten) toetsen wenst Opdrachtgever hiervoor een onafhankelijk A&P-testbedrijf in te zetten. Opdrachtnemer accepteert en werkt hier aan mee; hiervoor is het nodig dat de Opdrachtnemer een Vrijwaringsverklaring af geeft.

De precieze invulling van de A&P-test is afhankelijk van de situatie. Het kan een A&P-test zijn binnen de keten waar de ITSM-oplossing onderdeel van is. Het organiseren van deze A&P-test gebeurt door de Opdrachtgever en het uitvoeren van de A&P-test zelf is voor rekening van de Opdrachtgever.

Eventuele Kwetsbaarheden worden als onderdeel van Onderhoud & Support opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan.

UE 23.	Opdrachtnemer conformeert zich aan het meewerken aan een toets en hierboven, onder het kopje Inleiding genoemde, beschreven werkwijze.
--------	---

Vulnerability scans

Deze zijn bedoeld om geautomatiseerd te scannen op bekende Kwetsbaarheden. Een Vulnerability scan kan dus met een grote regelmaat worden uitgevoerd. De reden is dat aan de ene kant de ITSM-oplossing ge-update wordt en aan de andere kant hackers en beveiligingsonderzoekers constant op zoek zijn naar nieuwe Kwetsbaarheden.

Aanvullend kan de ITSM-oplossing tijdens het ontwikkelproces on-the-fly worden getest met daarvoor geschikte hulpmiddelen.

UE 24.	Opdrachtnemer voert minimaal maandelijks een Vulnerability scan uit op de ITSM-oplossing conform bovenstaande. Hierbij geldt dat de gebruikte tooling, waar Opdrachtnemer zelf in dient te voorzien, gebruik maakt van up-to-date kwetsbaarheiddefinitiesbestanden. Op verzoek worden testresultaten, zeker als ze gekwalificeerd zijn als Kritisch of Hoog, gedeeld met de Belastingdienst. Eventuele Kwetsbaarheden als onderdeel van Onderhoud & Support opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan.
--------	---

UE 25.	In aanvulling op UE 24 geldt dat de gebruikte tooling t.b.v. het uitvoeren van een Vulnerability scan, waar Opdrachtnemer zelf in dient te voorzien, gebruik maakt van up-to-date kwetsbaarheiddefinitiesbestanden. Op verzoek worden testresultaten, zeker als ze gekwalificeerd zijn als Kritisch of Hoog, gedeeld met de Belastingdienst. Eventuele Kwetsbaarheden worden als onderdeel van Onderhoud & Support opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan. Opdrachtnemer conformeert zich hier aan.
--------	---

UE 26.	Als Opdrachtgever het noodzakelijk acht, op basis van een risico inschatting, een Vulnerability scan uit te laten voeren op de ITSM-oplossing, dan staat Opdrachtnemer dat toe. De kosten van het uitvoeren van de Vulnerability scan worden gedragen door de Opdrachtgever. Eventuele Kwetsbaarheden worden als onderdeel van Onderhoud & Support opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan. Opdrachtnemer conformeert zich hier aan.
--------	---

Beveiligingstestbeleid

De Opdrachtgever wenst inzage in het beveiligingstestbeleid van Inschrijver. Het betreft opzet, bestaan en werking van de A&P-testen en Vulnerability scans. Hiertoe worden documenten aangeleverd waarin het beveiligingstestbeleid wordt beschreven en hoe eventuele tekortkomingen worden afgehandeld. Ook moet blijken onder welke omstandigheden dergelijke beveiligingstesten worden uitgevoerd en dat deze worden uitgevoerd. Hier maken ook voorbeelden van een A&P-testrapport en een Vulnerability testrapport deel van uit.

GUE 58.	Inschrijver beschikt over een beveiligingstestbeleid dat in bovenstaande informatiebehoefte voorziet.
---------	---

Dit beveiligingstestbeleid wordt in de verificatieperiode bij de beste Inschrijver opgevraagd.

3.2.8. Continuïteit en continuïteitstesten

Opdrachtgever vindt het van belang te weten welke maatregelen getroffen zijn om eventuele onbeschikbaarheid te voorkomen én mocht onbeschikbaarheid toch groter zijn dan gepland, hoe snel de Gegevens beschikbaar zijn dan wel de ITSM-oplossing weer volledig operationeel kan zijn. Het gaat hierbij dus niet om de beschikbaarheidseisen waar het vooral draait om wanneer de ITSM-oplossing wel of niet te gebruiken is, maar om de excepties dat het mis gaat.

Calamiteit

Een Calamiteit kan optreden als de Productie-omgeving, of de Gegevens daarop, volledig onbeschikbaar worden. In een dergelijke situatie mag er geen sprake zijn van inbreuk op Integriteit en Vertrouwelijkheid van de Gegevens. Opdrachtnemer is hierop voorbereid door het opstellen van een Calamiteitenplan (Disaster Recovery Plan).

Het is noodzakelijk minimaal 1x per jaar een test uit te voeren om te controleren of de ITSM-oplossing naar aanleiding van gesimuleerde noodsituaties kan worden hersteld en daarna kan blijven functioneren, zoals overeengekomen.

Opdrachtnemer werkt mee aan het implementeren van eventuele verbeterpunten die van toepassing zijn op de ITSM-oplossing zelf.

Afspraken hierover worden in een DAP met de Belastingdienst vastgelegd.

UE 27.	Opdrachtnemer conformeert zich aan bovenstaande alinea m.b.t. het uitvoeren en de uitkomsten van een Disaster Recovery Test.
--------	--

3.2.9. Monitoring, Alerting & Logging

De Opdrachtgever wil zicht hebben op afwijkingen op de werking van de ITSM-oplossing om herstelacties te kunnen formuleren en zo mogelijk in de toekomst te voorkomen. Denk aan (ongeautoriseerde) toegang tot de ITSM-oplossing, maar ook inzage, wijziging of verwijdering van Gegevens. Speciale aandacht voor gevoelige Gegevens, zoals Persoonsgegevens. Ook, bijvoorbeeld, financiële Gegevens kunnen extra aandacht nodig hebben.

De ITSM-oplossing (inclusief raakvlaksystemen en tooling) wordt volcontinu gemonitord op verstoringen en beveiligingsinbreuken zodat er direct adequaat gereageerd kan worden op (beveiligings)incidenten. Er is een alertingproces ingericht om direct (prio 1) te kunnen handelen in geval van incidenten en (dreigende) verstoringen.

Excepties, zoals bijvoorbeeld in geval van blokkerende applicatieve fouten, worden gelogd.

Beveiligingsinbreuken worden daarnaast gelogd voor forensisch onderzoek.

Inbreuken worden vastgelegd en acties worden genomen de ontstane risico's te mitigeren.

Logregels bevatten minimaal:

- Datum en tijd;
- IP-adres of hostnaam van het device dat de informatie logt;
- IP-adres van het remote systeem (indien met een ander systeem wordt gecommuniceerd);
- Identificatie van de gebruiker of het proces;
- Beschrijving van de activiteit of gebeurtenis;
- Het resultaat van de activiteit of gebeurtenis.

Gebeurtenissen die gelogd moeten worden zijn:

- Authenticatie/autorisatie pogingen, inloggen en uitloggen;
- Acties die betrekking hebben op gebruikersprofielen, bestanden en databases of systeemservices;
- Transacties tussen systemen;
- Activatie en/of de-activering van beveiligingsfunctionaliteit;
- Niet gespecificeerd gedrag van systemen en applicaties (uitzonderingen, fouten en storingen);
- Beveiligingsincidenten.

Logbestanden zijn beveiligd tegen ongeautoriseerde toegang/wijziging en zijn geschikt om forensisch onderzoek te verrichten. Logbestanden in het kader van technische beveiligingslogging worden minimaal

18 maanden bewaard. Logbestanden die onderdeel uitmaken van forensisch onderzoek naar een beveiligingsincident worden bewaard, zolang het onderzoek niet afgesloten is. Logregels bevatten geen informatie waarmee de beveiliging van de ITSM-oplossing gecompromitteerd kan worden

Via alerting wordt direct adequaat gereageerd op excepties om de situatie te onderzoeken en eventuele risico's te mitigeren. Onder excepties vallen ook incidenten rond ongeautoriseerde toegang en wijziging van logbestanden.

Afspraken hiervoor moeten worden beschreven in een DAP met de Belastingdienst.

GUE 59. De ITSM-oplossing voldoet aan de voorwaarden zoals beschreven in bovenstaande alinea's.

UE 28. Opdrachtnemer levert op verzoek inzicht in de logging.

GUE 60. De ITSM-oplossing ondersteunt het instellen van loglevels en onderscheidt hier minimaal info-, error- en fatal-meldingen in.

GUE 61. De ITSM-oplossing biedt de mogelijkheid om na een foutsituatie Gegevens te herstellen zodat de gebruiker zijn/haar werk kan hervatten.

3.2.10. Autorisatie & Authenticatie

GUE 62. Voor authenticatie sluit de ITSM-oplossing aan op de Belastingdienst Active Directory via een SAMLv2/OpenID Connect aansluiting op de Federated Identity Hub.

GUE 63. De communicatie over het netwerk van de wachtwoorden van gebruikers in relatie met de ITSM-oplossing is versleuteld.

Toegang tot ITSM-oplossing en Gegevens van de Aanbestedende dienst vindt plaats op basis van need-to-know en least privilege. Anders gezegd: gebruikers van zowel Opdrachtgever als Opdrachtnemer krijgen alleen die rechten die nodig zijn voor het uitoefenen van hun vastgestelde taken voor wat betreft Gegevens en functionaliteit van de ITSM-oplossing. Dit is overigens ook van toepassing op raakvlaksystemen (koppelende applicaties).

Een belangrijk aspect hierbij is dat de technische Beheerders geen toegang krijgen tot data in de Productieomgeving.

De ITSM-oplossing is technisch zodanig ingericht zodat deze principes zijn voldaan.

GUE 64. De ITSM-oplossing voldoet aan wat in bovenstaande alinea is beschreven.

GUE 65. De ITSM-oplossing bevat maatregelen om ongeautoriseerde toegang tot de ITSM-oplossing uit te sluiten.

Hoofdstuk 4. Integriteit

4.1. Business Etiquette

Opdrachtgever maakt graag gebruik van de kennis en innovatieve kracht uit de markt. Daarvoor werkt de Opdrachtgever samen met leveranciers. In deze samenwerking speelt u dus een essentiële rol. Opdrachtgever vindt onpartijdigheid en transparantie belangrijk. Daarom maken we afspraken hierover: onze Business Etiquette.

UE 29.	Opdrachtnemer conformeert zich aan de Business Etiquette zoals opgenomen in Bijlage 4 van het Beschrijvend Document versie 1.2 .
--------	--

Hoofdstuk 5. Maatschappelijk Verantwoord Inkopen (MVI)

De Belastingdienst heeft ambitie op het gebied van duurzaamheid. Zij wil klanten, behoeftebestellers en leveranciers begeleiden in het vormgeven van de duurzaamheidsaspecten in producten en diensten op het vlak van bedrijfsvoering, bij aanbestedingen en gedurende de looptijd van de contracten (maatschappelijk verantwoord inkopen).

Maatschappelijk Verantwoord Inkopen (MVI) binnen de overheid is een uitvloeisel van een politiek besluit. Sinds 2010 is de rijksoverheid verplicht 100% duurzaam in te kopen. Door gelijktijdig milieu-, sociale- en economische afwegingen in alle aankopen mee te nemen leidt dit tot winst voor de belastingbetaler, de overheidsorganisatie en de samenleving.

Het nieuwe regeerakkoord stelt dat de overheid zijn inkoopkracht beter gaat benutten voor het versnellen van duurzame transities, inschakelen van kwetsbare groepen en om innovatief in te kopen.

Hoe de Belastingdienst MVI wil toepassen op deze opdracht vindt u in de volgende paragrafen. Hierin zijn de toepasselijke MVI thema's beschreven.

5.1. Energie & Klimaat

Onder dit thema vallen onder andere:

- Energiegebruik;
- CO₂ reductie en
- Duurzame energie opwekking

100% CO₂-compensatie dienstreizen

Nederland moet voor 2030 de helft minder CO₂ uitstoten ten opzichte van 1990, en in 2050 95% procent minder. In het klimaatakkoord staan de maatregelen die sectoren de komende 10 jaar nemen om de doelen voor CO₂-reductie te halen.

Het klimaatakkoord is een onderdeel van het Nederlandse klimaatbeleid. Het is een overeenkomst tussen veel organisaties en bedrijven in Nederland om de uitstoot van broeikasgassen tegen te gaan. Daarmee wordt de opwarming van de aarde beperkt.

Bron: <https://www.rijksoverheid.nl/onderwerpen/klimaatverandering/klimaatakkoord/wat-is-het-klimaatakkoord>

De Inschrijver kan hier aan bijdragen door o.a. door de vrijgekomen CO₂ vanwege dienstreizen van medewerkers van de Inschrijver voor 100% te compenseren.

W 5	Geef aan of alle vrijgekomen CO₂ vanwege dienstreizen van medewerkers van de Inschrijver 100% gecompenseerd wordt. Alleen CO₂-credits worden geaccepteerd waarvoor de CO₂-reductie is gerealiseerd conform de richtlijnen van de CDM methodologie. Het Clean Development Mechanism (CDM) stelt eisen aan het vastleggen van de uitgangssituatie en aan de monitoring van een CDM mitigatie project met als doel de hoeveelheid Certified Emission Reductions (CER's) veroorzaakt door het project te bepalen. Deze methodologie is ook van toepassing op Verified Emission Reductions (VER's) en Emission Reduction Units (ERU's). Onder CO₂-compensatie wordt verstaan: het compenseren van vrijgekomen broeikasgassen (vertaald naar CO₂-equivalenten) door het vastleggen van CO₂ in bomen of het voorkomen van CO₂-uitstoot door het investeren in duurzame energie en/of energiebesparing. Voor CO₂-emissiefactoren voor buitenlandse dienstreizen gelden de waarden (well-to-wheel) zoals opgenomen op de website CO₂emissiefactoren.nl. De berekeningsmethodiek voor de vliegafstand wordt bepaald m.b.v. de IATA-code tabel. De beoordelingscriteria voor deze Wens is: <table> <tr> <td>Alle vrijgekomen CO₂ vanwege dienstreizen wordt 100% gecompenseerd</td><td>55 punten</td></tr> <tr> <td>Niet alle vrijgekomen CO₂ vanwege dienstreizen wordt 100% gecompenseerd</td><td>0 punten</td></tr> </table> De Inschrijver toont met een onderstaande mogelijke bewijsmiddelen aan dat aan het criterium is voldaan:	Alle vrijgekomen CO ₂ vanwege dienstreizen wordt 100% gecompenseerd	55 punten	Niet alle vrijgekomen CO ₂ vanwege dienstreizen wordt 100% gecompenseerd	0 punten
Alle vrijgekomen CO ₂ vanwege dienstreizen wordt 100% gecompenseerd	55 punten				
Niet alle vrijgekomen CO ₂ vanwege dienstreizen wordt 100% gecompenseerd	0 punten				

- Een Gold Standard certificaat (Informatie over Gold Standard is verkrijgbaar via goldstandard.org (Engelstalig));
- Een ander gelijkwaardig certificaat;
- Een ander gelijkwaardig bewijsmiddel.

Als er geen bewijs wordt ingediend, worden er geen punten toegekend.

Duurzame energieopwekking

Op de website van PIANOo zijn voorbeelden gegeven met betrekking tot het gebruik van energie uit duurzame bronnen: <https://www.piano.nl/themas/maatschappelijk-verantwoord-inkopen/mvi-criteria/productgroep-energie>.

Hieruit is de volgende Wens ontstaan:

W 6 Geef aan in welke mate het datacenter waarin de Cloud variant van de ITSM-oplossing gehost wordt CO₂ neutraal is.

Het beoordelingscriterium voor deze Wens is:

Van 96 % tot en met 100%	370 punten;
Van 91 % tot 95%	222 punten;
Van 81 % tot 90%	148 punten;
Van 71 % tot 80%	93 punten;
Van 61 % tot 70%	55 punten;
Van 51 % tot 60%	18 punten;
Van 41 % tot 50%	7 punten;
Van 0 % tot 40%	0 punten.

De Inschrijver toont dit met een bewijs aan waaruit blijkt dat aan dit criterium is voldaan.

Als er geen bewijs wordt ingediend, worden er geen punten toegekend.

5.2.

Welzijn & Gezondheid

De Belastingdienst heeft het welzijn en gezondheid van eigen personeel hoog in het vaandel. Dit wordt dan ook van de Opdrachtnemer en, indien van toepassing, zijn toeleveranciers verwacht. De inschrijver wordt daarom verzocht te omschrijven op welke wijze dit is ingericht.

W 7 Beschrijf in maximaal 2 A4 op welke wijze Inschrijver zorg draagt voor de welzijn en gezondheid van zijn werknemers.

Het beoordelingscriterium voor deze Wens is:

Medezeggenschap van de medewerker is geregeld	51 punten;
Er zijn stimulerende maatregelen getroffen die bijdragen aan de gezondheid van de werknemer	24 punten;
Geen van bovengenoemde onderdelen	0 punten.

Op deze Wens kunnen maximaal 75 punten worden behaald.

5.3.

Social Return on Investment

Als onderdeel van het maatschappelijk verantwoord ondernemen heeft de Rijksoverheid beleidsdoelstellingen geformuleerd ten aanzien van social return. De Rijksoverheid kiest voor maatregelen die eraan bijdragen dat iedereen zoveel mogelijk participeert in de samenleving en om mensen perspectief te bieden op werk en inkomen. Voor wie dit niet op eigen kracht kan, heeft de overheid de taak ondersteuning te geven om tot de arbeidsmarkt toe te treden. Het toepassen van social return past hierin. Met de toepassing van social return zorgt de Rijksoverheid ervoor dat elke investering die binnen het Rijk wordt gedaan, naast het 'gewone' rendement, een concrete, sociale winst oplevert.

Social return heeft tot doel het creëren van extra (leer)werkplekken, boven op de bestaande formatie. Het gehanteerde percentage is daarmee geen quotum, zodat mensen met een beperking die reeds werkzaam zijn bij de Inschrijver niet meetellen.

De gehele overheid (Rijk, provincies, waterschappen en gemeenten) doet de laatste jaren steeds meer ervaring op met het leveren van een bijdrage aan deze doelstelling. Door social return op te nemen in aanbestedingen binnen de categorie 'werken' en 'diensten' met een loonsom hoger dan € 250.000,00 exclusief BTW, wil de Rijksoverheid een extra impuls geven aan social return.

Opdrachtnemer dient bij de uitvoering van de opdracht aan social return bij te dragen door het creëren van extra werk(ervarings)plaatsen voor mensen met een grote(re) afstand tot de arbeidsmarkt. Voor deze aanbesteding wordt uitgegaan dat minimaal 5% van het totale aantal in te zetten uren van de Overeenkomst wordt ingezet voor de doelgroep.

Voorafgaand aan het sluiten van de Overeenkomst wordt afgestemd op welke wijze Opdrachtnemer invulling geeft aan social return en hoe de invulling geverifieerd kan worden door de Opdrachtgever.

UE 30.	Tijdens de looptijd van de Overeenkomst besteedt de Opdrachtnemer gedurende de looptijd van de Overeenkomst minimaal 5% van het totaal afgenomen Consultancy en Opleidingen ex. BTW per jaar aan extra werk(ervarings)plaatsen voor mensen uit genoemde social return doelgroepen.
UE 31.	Na het tekenen van de Overeenkomst stemmen Partijen met elkaar af over de wijze waarop invulling wordt gegeven aan social return.
UE 32.	Opdrachtnemer stuurt aan de Opdrachtgever elk half jaar, uiterlijk 15 kalenderdagen na ommekomst van deze periode, geheel ingevuld en ondertekend een periodiek verantwoordingsformulier social return toe. Dit periodiek verantwoordingsformulier social return is opgenomen als Bijlage 3 bij de Overeenkomst.
UE 33.	Wanneer op basis van de periodieke verantwoordingsformulieren de Opdrachtgever constateert dat de Opdrachtnemer gedurende de looptijd van de Overeenkomst tweemaal achtereenvolgend niet aan de verplichting voldoet zoals beschreven in UE 30, dan kan de Opdrachtnemer in overleg treden met Opdrachtnemer. Op basis van dit overleg: - Stellen Partijen de oorzaken vast voor het niet behalen van het genoemde percentage door de Opdrachtnemer; - Stelt Opdrachtgever maatregelen vast voor het verbeterd nakomen van de verplichting tot social return door de Opdrachtnemer.
UE 34.	Bij het niet nakomen van de verplichting genoemd in UE 30, kan de Opdrachtgever naar rato van de bijdrage social return die de Opdrachtnemer moest doen, betalingen inhouden of storneren op de waarde van de Overeenkomst, met uitzondering in die situaties dat het voldoen aan de verplichting genoemd in UE 30 buiten de schuld van de Opdrachtnemer om niet lukt(e). De bewijslast rust te allen tijde bij de Opdrachtnemer.

5.4. Internationale sociale voorwaarden

Internationale verdragen bevatten morele normen over mensenrechten, arbeidsomstandigheden en beloningen. Het voldoen aan sociale aspecten van duurzaam inkopen betekent dat leveranciers zich moeten inspannen dat deze normen in de hele keten van het productieproces worden nagestreefd. De systematiek die hiervoor is ontworpen, noemen we 'sociale voorwaarden'. De fundamentele normen in de verdragen van Internationale Arbeidsorganisatie en de normen in de Universele Verklaring van de Rechten van de Mens, noemen we generieke normen. Zij gelden voor de inkoop van alle producten. Voor sommige productgroepen heeft de Rijksoverheid aanvullende normen gesteld. Met aanvullende normen streven we in die producten een nog grotere verbetering na van arbeidsomstandigheden en beloningen.

Op deze opdracht zijn de generieke sociale voorwaarden van toepassing.

De ingevulde en ondertekende bijlage sociale voorwaarden maakt onderdeel uit van de Overeenkomst.

GUE 66.	Inschrijver zal de sociale voorwaarden (Bijlage 3) op eerste verzoek van de Aanbestedende dienst, maar niet eerder dan na het mededelen van de gunningsbeslissing, invullen en ondertekend aanleveren.
UE 35.	Opdrachtnemer dient rekening te houden met de verplichtingen uit hoofde van de bepalingen inzake de arbeidsbescherming en de arbeidsvoorwaarden die gelden in het land waar de opdracht wordt uitgevoerd, zoals bedoeld in artikel 2.81 lid 2 Aw2012. Kennis omtrent die belastingen en milieubescherming, arbeidsvoorwaarden en arbeidsbescherming kunnen Inschrijvers, voor zover het gaat om uitvoering in Nederland, verkrijgen bij: • Opdrachtgever, www.belastingdienst.nl; • Het Ministerie van Infrastructuur en Waterstaat, https://www.rijksoverheid.nl/ministeries/ministerie-van-infrastructuur-en-waterstaat; • Het Ministerie van Sociale Zaken en Werkgelegenheid, www.rijksoverheid.nl/ministeries/szw.

Hoofdstuk 6. Juridische kaders

Concept Overeenkomst

De in Bijlage 2 van het Beschrijvend Document versie 1.2 opgenomen concept Overeenkomst kan - alvorens deze door Inschrijver(s) wordt ondertekend - door de Aanbestedende dienst worden gewijzigd en nader uitgewerkt, mede naar aanleiding van de door de Inschrijver gedane opmerkingen en tekstsuggesties als bedoeld in paragraaf 3.2.1. (Nadere inlichtingen of vragen over de aanbestedingsstukken). De wijzigingen en/of de aangepaste overeenkomst zullen/zal de Inschrijvers per nota van inlichtingen kenbaar worden gemaakt.

GUE 67.	Inschrijver gaat akkoord met de concept Overeenkomst met inbegrip van de eventuele per Nota van Inlichtingen kenbaar gemaakte wijzigingen zoals genoemd in deze paragraaf.
---------	--

Gedurende de looptijd van de Overeenkomst is een Service Level Agreement (SLA) van toepassing waarin afspraken over verantwoordelijkheden, kwaliteit en beschikbaarheid tussen Opdrachtnemer en Opdrachtgever zijn beschreven. Dit gebeurt op basis van (meetbare) prestatie-indicatoren en kwaliteitseisen.

Hoe de Opdrachtnemer en de Opdrachtgever samenwerken wordt vastgelegd in een Dossier Afspraken en Procedures (DAP). Op basis van de SLA wordt maandelijks gerapporteerd door Opdrachtnemer. Dit gebeurt via een Service Niveau Rapportage (SNR).

Activiteiten die om redenen niet binnen de termijn kunnen worden opgelost worden opgenomen in een Verbeterplan.

Voor deze aanbesteding is niet gekozen om een template SLA en DAP mee te sturen, maar deze gezamenlijk na ingang van de Overeenkomst op te stellen. In paragraaf 10.1 staat hierover meer informatie.

GUE 68.	Inschrijver gaat akkoord met de werkwijze om pas na gunning gezamenlijk een SLA en DAP inclusief gevraagde procedures op te stellen.
---------	--

De Aanbestedende dienst vindt het van belang dat zijn Gegevens veilig zijn. Gegevens moeten beschikbaar zijn, maar ook betrouwbaar (niet onbevoegd gewijzigd) en alleen toegankelijk voor de personen die die Gegevens daadwerkelijk nodig hebben.

Gegevens dienen verwerkt (onder andere: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen) te worden in de EU en landen waarvan de Europese Commissie bepaald heeft dat in deze landen een passend beveiligingsniveau is.

Zie hiervoor: <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal/doorgifte-binnen-en-buiten-de-eu#hoe-weet-ik-of-een-derde-land-een-passend-beschermingsniveau-heeft-1752>

GUE 69.	Inschrijver verklaart dat Gegevens alleen worden verwerkt in lidstaten van de EU of een land met een door de EU goedgekeurd beveiligingsniveau én deze landen niet verlaten. Inschrijver levert het bewijs aan als Bijlage XII van de Inschrijving.
---------	--

UE 36.	Opdrachtnemer heeft (technische) maatregelen getroffen om te voorkomen dat Gegevens van de Opdrachtgever geleverd (kunnen) worden aan andere partijen die niet onder Nederlandse of Europese wetgeving vallen.
--------	--

Hoofdstuk 7. Prijsstelling

7.1. Algemene eisen ten aanzien van Prijzen

In de in Bijlage VIII “Prijzenformulier versie 1.1” geoffreerde Prijzen dienen alle kosten voor de ITSM-oplossing of Prestatie verdisconteerd te zijn. Deze kosten kunnen door Opdrachtnemer niet verbijzonderd worden verrekend aan Opdrachtgever. Hierbij kan (en niet limitatief) worden gedacht aan:

- Periodieke rapportages;
- Periodiek overleg;
- Inspecties;
- Evaluaties;
- Toekomstverkenningen;
- Deelname aan begeleidings- en stuurgroepen;
- Reis- en verblijfkosten;
- Het verstrekken van de benodigde toegangscodes voor gebruik van de ITSM-oplossing;
- Materialen en Documentatie vereist voor het gebruik van de ITSM-oplossing.

UE 37.	Kosten die niet in de Inschrijving genoemd worden en niet verdisconteerd zijn in de Prijzen, maar toch noodzakelijk blijken te zijn voor een optimaal functioneren van de Prestatie conform de in de Aanbestedingsstukken gestelde eisen én de in de Inschrijving opgenomen beantwoording van de wensen, kan Opdrachtnemer niet in rekening brengen bij Opdrachtgever.
GUE 70.	Eventuele valutarisico's zijn volledig voor rekening van Opdrachtnemer en worden geacht in de geoffreerde Prijzen te zijn verwerkt.
GUE 71.	Alle geoffreerde tarieven met betrekking tot de Additionele diensten (Consultancy en Opleidingen) zijn inclusief reis- en verblijfkosten.
UE 38.	Voor zover Opdrachtnemer gehouden is omzetbelasting in rekening te brengen, zullen de in het Prijzenformulier vermelde bedragen worden verhoogd met het geldende percentage omzetbelasting.

7.2. Toelichting Prijscomponenten in Bijlage VIII “Prijzenformulier, versie 1.1”

Het Prijzenformulier is uit verschillende tabbladen opgebouwd. Voor alle tabbladen geldt dat de gele invulvelden ingevuld moeten worden. Hieronder volgt per tabblad een uitleg/toelichting

Let op! De Aanbestedende dienst beseft dat het onmogelijk is Prijzen en/of Tarieven voor 14 jaar af te geven. Voor het bepalen van de Vergelijkingswaarde moet Inschrijver bij het invullen van het Prijzenformulier uitgaan van de huidige Prijzen en/of Tarieven.

Tabblad Samenvatting

In dit tabblad vult de Inschrijver alleen de naam in; alle overige cellen worden automatisch vanuit de verschillende tabbladen ingevuld.

Tabblad ITSM versus practices & integraties

In dit tabblad vult de Inschrijver in de gele velden welke onderdelen van de ITSM-oplossing de betreffende practice/integratie is opgenomen. Uit de eerder gehouden RFI is naar voren gekomen dat hier verschillen in zitten.

In de kolom ‘Modules’ vult Inschrijver de namen van de aangeboden componenten in; in de kolommen D tot en met W vult Inschrijver in de betreffende cel een ‘X’ of ‘✓’ in als deze onderdeel uitmaakt van het betreffende component. Het kan voorkomen/is toegestaan dat bij een Module een ‘X’ of ‘✓’ in één of meerdere ITILv4 practices en/of integraties geplaatst worden.

Tabblad Dimensionering

In dit tabblad zijn geen invulvelden.

Dit tabblad dient als input voor de overige tabbladen.

Met betrekking tot de dimensionering van gebruikers geldt dat de Behandelaren en goedkeurders/raadplegers in de Ontwikkel-, Test- en Acceptatieomgeving genoemd, dezelfde unieke Behandelaren zijn als in de Productieomgeving. Voor jaar 1 geldt dus het totaal aantal Behandelaren over de gehele OTAP maximaal 100 is.

Tabblad 1 Subscriptions

In dit tabblad vult Inschrijver op basis van de dimensionering in dit tabblad én de overige dimensionering van het tabblad Dimensionering in de gele cellen de kosten per jaar en een eventueel kortingspercentage in. Daarnaast is het mogelijk overige kosten op te voeren.

Let op!

Bij dit tabblad moet Bijlage VIIIb Toelichting Prijzenformulier worden ingediend met daarin een duidelijke toelichting op de ingevulde bedragen.

Tabblad 2 Additionele Diensten

Consultancy

Inschrijver vult m.b.t. de Consultancy in de cellen C19 tot en met C21 een dagtarief in.

Het totaal van alle kosten per jaar wordt automatisch opgeteld en in cel C23 weergegeven en naar cel D17 van het tabblad 'Samenvatting' gekopieerd.

Bonus/malus; zie ook Tabblad Factor

Voor de Aanbestedende dienst is een marktconforme prijsstelling belangrijk. Daarom past de Aanbestedende dienst in deze aanbesteding een methode toe waarbij een fictieve bonus/ malus wordt verkregen op basis van geoffreerde uurtarieven. Omdat de berekening van de fictieve bonus/ malus plaatsvindt op basis van een algoritme zijn de dagtarieven zoals ingevuld in de cellen C19 tot en met C21 omgerekend naar een uurtarief; deze zijn in de cellen F32 tot en met F34. De berekening is geheel geautomatiseerd; Inschrijver hoeft hiervoor niets in te vullen.

Bij een geoffreerd tarief lager dan de referentieprij wordt een fictieve bonus verkregen. Bij een geoffreerd tarief hoger dan de referentieprij wordt een fictieve malus verkregen. De fictieve bonus/ malus is progressief variabel en is vastgesteld op maximaal 10%. De fictieve bonus/ malus heeft invloed op de Vergelijkingswaarde van Inschrijver. Gedurende de looptijd van de Overeenkomst vindt verrekening plaats op basis van de door Inschrijver geoffreerde tarieven **exclusief** de bonus/ malus. Het tabblad "Factor" geeft inzicht in de hoogte van de bonus/ malus.

De berekende bonus/ malus wordt in cel N34 getoond en naar cel C25 én naar cel D18 van het tabblad 'Samenvatting' gekopieerd.

Tabblad Factor

Het tabblad "Factor" geeft inzicht in de hoogte van de bonus/ malus. Inschrijver hoeft in dit tabblad niets in te vullen.

Opleiding

Inschrijver vult m.b.t. de Opleiding op gegevens van een opleiding/training in voor 10 functioneel beheerders.

Inschrijver heeft hierbij de mogelijkheid een kortingspercentage aan te bieden, de groepsgrootte en het aantal sessies te bepalen. De voorkeur gaat uit naar één sessie.

Als deze Opleiding/training kosteloos wordt aangeboden, dient Inschrijver de waarde 'o' (nul) bij de prijs in te vullen

Het totaal van alle kosten per jaar wordt automatisch opgeteld en naar cel D19 van het tabblad 'Samenvatting' gekopieerd.

Tabblad BPK-grafiek

In cel F9 is het totaal van de cel D23 van het tabblad 'Samenvatting' overgenomen.

Inschrijver kan in cel F12 een eigen inschatting invullen om te zien hoe de aangegeven waarde van de Inschrijving zich verhoudt tot de inschatting van de Aanbestedende dienst.

Let op! De werkelijke score van de kwaliteit wordt bepaald door de Aanbestedende dienst.

7.3. Specifieke eisen ten aanzien van Prijzen

Omdat in het Prijzenformulier voor de Subscriptions alleen de kosten per jaar moeten worden aangegeven, is er geen inzicht in het afrekenmodel van de Inschrijver. Omdat de Overeenkomst lang loopt en niet meteen de volle omvang van de dimensionering wordt afgenomen én deze informatie wel gewenst is, wordt van Inschrijver verwacht uit toelichting bij de Inschrijving in te dienen.

In de toelichting moeten de navolgende zaken beschreven worden:

- Soorten grondslagen waarop wordt afgerekend;
- Staffels;
- Wel of geen onderscheid in het gebruik van de ITSM-oplossing voor productie en/of test omgevingen

GUE 72.	Inschrijver levert op basis van bovenstaande als Bijlage VIIIb een toelichting bij het Prijzenformulier (Bijlage VIII, versie 1.1) bij de Inschrijving in. Zowel tekstueel als rekenkundig moet expliciet en duidelijk en eenduidig herleidbaar te zijn hoe de jaarbedragen in verhouding staan met de genoemde dimensionering en de in het tabblad "Dimensionering" gegeven uitgangspunten. Hierbij moet onder andere gedacht worden aan de grondslag(en) van de aangeboden Subscriptions /Gebruiksrechten, de gebruikte staffels met aantallen, prijsstellingen per eenheden (staffel) en de benodigde aantallen en hoe deze correleren met de aangegeven dimensionering. Hierbij is ook een mogelijkheid om een Subscription/ Gebruiksrecht, aan te bieden voor bijvoorbeeld Onbeperkt gebruik. Let op! Voor staffels geldt dat de Prijs van een Subscription/ Gebruiksrecht van de opvolgende staffel minimaal gelijk of lager moet zijn dan de voorgaande staffel.
GUE 73.	Het is niet toegestaan om negatieve Prijzen die de gehanteerde berekeningen frustreren of die bij voorbaat objectief niet afzonderlijk kunnen worden nagekomen, te offeren.

7.4. Indexering Prijs

De door Inschrijver geoffreerde Prijzen zoals opgegeven in het spreadsheet Prijzenformulier versie 1.1, Bijlage VIII, mogen vanaf 2025 jaarlijks en steeds per jaarlijkse verlengdatum geïndexeerd worden op basis van de CBS tabel 'CAO-lonen, contractuele loonkosten en arbeidsduur, indexcijfers (2010 = 100)'; onderwerp: CAO- lonen incl. bijz. beloningen; SBI2008: M-N Zakelijke dienstverlening, of de opvolger van deze index, conform de volgende webpagina:

<https://opendata.cbs.nl/statline/#/CBS/nl/dataset/82838NED/table?dl=74C6F>

De door Inschrijver geoffreerde Prijzen voor het Gebruiksrecht zoals opgegeven in het spreadsheet Prijzenformulier versie 1.1, Bijlage VIII, in tabbladen '1a...', '1b...' en '1c...' mogen vanaf 2025 jaarlijks en steeds jaarlijkse verlengdatum geïndexeerd worden op basis van de CBS-tabel Dienstenprijzen (DPI); commerciële dienstverlening en transport; indexcijfers 2015 = 100 (CPA2008, kwartaalindex), of de opvolger van deze index, conform de volgende webpagina:

<https://opendata.cbs.nl/#/CBS/nl/dataset/83760NED/table?dl=74C78>

Prijsaanpassingen dienen uiterlijk twee maanden voor het verlengingsmoment aan de contractmanager ter goedkeuring te worden aangeboden, waarbij het op dat moment – door het CBS – meest recent beschikbare en gepresenteerde indexcijfer, Jaarmutatie per kwartaal, gehanteerd wordt. Het percentage voor de tariefstijging wordt afgerond op één decimaal achter de komma. Inhaalslagen op niet doorgevoerde indexeringen worden niet geaccepteerd.

Voorbeeld: als de overeenkomst voor de tarieven van Consultancy op 1 september 2022 geïndexeerd had mogen worden, was de prijsindexatie 2,8% geweest (jaarmutatie DPI 2e kwartaal 2022, op dat moment meest recent beschikbare indexcijfer).

UE 39.	De door de Opdrachtnemer geoffreerde Prijzen mogen jaarlijks per 1 augustus geïndexeerd worden conform paragraaf 7.4. De eerste indexering vindt plaats niet eerder dan 2 jaar na ingaan van de Overeenkomst.
UE 40.	Opdrachtnemer dient 2 maanden voorafgaande aan de genoemde momenten van indexering, een schriftelijk verzoek in met bijbehorende onderbouwing om voor de indexering in aanmerking te komen.

Hoofdstuk 8. Documentatie, Opleiding en Consultancy

8.1. Documentatie

UE 41.	Opdrachtnemer zal Opdrachtgever tijdig voorzien van actuele en volledige Documentatie in elektronische vorm met betrekking tot het gebruik van de Prestatie. Hierbij is de Documentatie over de eigenschappen en gebruiksmogelijkheden van de ITSM-oplossing in de Nederlandse en/of Engelse taal.
UE 42.	De Documentatie dient zodanig te zijn dat zij een juiste, volledige en gedetailleerde beschrijving geeft van de door Opdrachtnemer te leveren ITSM-oplossing en de functies daarvan, zodat Eindgebruikers gebruik kunnen maken van alle mogelijkheden van de ITSM-oplossing.
UE 43.	De eventueel specifiek voor de Opdrachtgever opgestelde Documentatie dient in een bewerkbaar format aangeleverd te worden, zodat Opdrachtgever deze zelf kan aanpassen wanneer Opdrachtgever in de toekomst zaken wijzigt in de Inrichting van de ITSM-oplossing.
UE 44.	Opdrachtgever mag de Documentatie voor gebruik binnen de eigen organisatie reproduceren en wijzigen.
UE 45.	Opdrachtnemer zal de door hem geleverde Documentatie zo spoedig mogelijk vervangen, wijzigen of aanpassen indien op enig tijdstip tijdens het gebruik door Opdrachtgever van de Prestatie, blijkt dat de Documentatie onjuiste informatie bevat of anderszins onvolledig, onvoldoende, onduidelijk en/of verouderd is.
UE 46.	Opdrachtnemer is verantwoordelijk dat Documentatie na een nieuwe Release actueel blijft. Na oplevering van een nieuwe Release wordt de geactualiseerde Documentatie digitaal beschikbaar gesteld.
UE 47.	Opdrachtnemer geeft in de Documentatie de in de Release opgenomen aanpassingen duidelijk weer.

8.2. Opleiding

UE 48.	Opdrachtnemer levert relevante Opleidingen, inclusief Documentatie, inzake het gebruik van de ITSM-oplossing, alsmede het functioneel beheer van de ITSM-oplossing.
UE 49.	Opleidingen vinden plaats op locatie van de Opdrachtgever tenzij nadrukkelijk anders overeengekomen.
UE 50.	De Opleidingen vinden plaats in Nederland in de Nederlandse taal.
UE 51.	Opdrachtnemer stelt voor de Eindgebruikers de goedgekeurde gebruikersinstructie online beschikbaar gedurende de looptijd inclusief verlengingsopties van de Overeenkomst en houdt deze actueel.
UE 52.	Opleiding en ondersteuning dient door deskundigen, die daartoe bekwaam en geschikt zijn, te worden gegeven. In voorkomend geval kan Opdrachtgever voorafgaand aan de inzet van de betreffende deskundige(n), overlegging van, of inzage in, relevante diploma's en/of certificaten vorderen.
UE 53.	Lesmateriaal voor de gebruikers van de ITSM-oplossing is in de Nederlandse en/of Engelse taal beschikbaar.

8.3. Consultancy

UE 54.	Consultants die ingezet worden voor werkzaamheden voldoen minimaal aan het profiel zoals beschreven in Bijlage 6 Rolbeschrijvingen, versie 1.1.
--------	---

Hoofdstuk 9. Beschikbaar stellen en Inrichten

9.1. Inrichting en beschikbaarstelling

De Opdrachtgever voorziet 2 soorten inrichting; technisch en functioneel.

Opdrachtnemer is (primair) verantwoordelijk voor de technische Inrichting.

Opdrachtgever is (primair) verantwoordelijk voor de functionele Inrichting, maar voorziet wel dat hiervoor ondersteuning van Opdrachtnemer noodzakelijk is.

Na het contracteren moet, conform het definitieve Plan van Aanpak, als eerste stap de ITSM-oplossing ingericht en beschikbaar worden gesteld.

Dit resulteert uiteindelijk in een OTAP-straat waarop de ITSM-oplossing gereed is voor het functioneel Inrichten van initiële configuratie en Migratie.

De ITSM-oplossing is na afronding van deze fase in gebruik én voldoet aan de SLA-eisen. De Acceptatie vindt plaats door medewerkers van team Tooling (de functioneel beheerders) en vertegenwoordigers van de gebruikersorganisatie.

De Opdrachtgever wil hierbij (zo veel mogelijk) geadviseerd en (optioneel) ondersteund worden in het op de beste en meest efficiënte manier m.b.t. de functionele Inrichting, Migratie en integratie van de ITSM-oplossing met te koppelen systemen/ omgevingen.

W 8 Met betrekking tot bovenstaande alinea's vraagt Opdrachtnemer een plan van aanpak waarin Inschrijver beschrijft hoe de oplossing beschikbaar gesteld wordt en de voorwaarden worden ingericht om veilig te kunnen koppelen, de oplossing het meest effectief kan worden ingericht evenals de Migratie van ICD naar de aangeboden ITSM-oplossing. Geef een uitgebreide en betrouwbare inschatting van het beschikbaar stellen, de functionele Inrichting, de acceptatie en de Migratie. Voor de opdrachtgever is het belangrijk dat de Migratie uiterlijk half 2026 is afgerond, er een goede geïntegreerde basis staat die doorontwikkeling mogelijk maakt en dat de nieuwe oplossing wordt geaccepteerd door de verschillende gebruikersgroepen.

Het plan bevat minimaal de volgende onderwerpen:

- Inhoudelijke aanpak om te komen tot een werkende ITSM-oplossing gekoppeld aan de infrastructuur van de Belastingdienst;
- Een duidelijke projectfasering die een beheerste control op de voortgang mogelijk maakt;
- Een aanpak die erin voorziet om in stappen (Agile) over te gaan van de oude naar de nieuwe ITSM-oplossing;
- Een duidelijke opzet t.a.v. projectgovernance die aansluit op de geschetste werkwijze;
- Verwachte bijdrage van Opdrachtgever om veilig systemen vanuit de Belastingdienst te kunnen koppelen aan de ITSM-oplossing;
- Inschatting van de benodigde inzet (projectmanagement, architect, BizDevOps engineer) per deliverable/projectonderdeel, waarbij tevens doorlooptijden worden aangegeven;
- Beschrijving van een helder acceptatieproces, waarbij acceptatie altijd door Opdrachtgever gebeurt op basis van positief verlopen acceptatietesten;
- De beschrijving van de 5 belangrijkste risico's en de maatregelen die Inschrijver voorstelt om deze risico's te beheersen.

Het plan van aanpak is, exclusief voorblad, inhoudsopgave en afbeeldingen, [maximaal 10 pagina's](#). Hyperlinks en/of verwijzingen naar andere documenten en/of websites zijn niet toegestaan.

Voor deze Wens geldt de volgende waardering:

- | | |
|-------|--------------|
| 0 | Zeer slecht; |
| 48 | Slecht; |
| 243 | Matig; |
| 405 | Voldoende; |
| 1.053 | Goed; |

1.620	Uitstekend.
LET OP!!! Op deze Wens moet er minimaal een score 'Voldoende' worden behaald. Dit is een knock out criterium Als het antwoord op de Wens een Matig of minder scoort, dan leidt tot uitsluiting van de aanbestedingsprocedure.	

9.2. Documentatie, Opleiding en Consultancy

UE 55.	Opdrachtnemer levert gedurende de voorbereidings- en implementatiefase van de Overeenkomst Documentatie, Opleiding en Consultancy conform de eisen zoals neergelegd in Hoofdstuk 8 'Documentatie, Opleiding en Consultancy'.
--------	--

9.2.1. Opleiding

UE 56.	Opdrachtnemer geeft op aanvraag van Opdrachtgever aan iedere doelgroep, werkzaam in de organisatie van Opdrachtgever (een) passende Opleiding(en) bestaande uit concrete invulling, zoals opleiding, cursus, instructie, product sessies/seminars, etc.
UE 57.	In geval van uitstel of vertraging van het beschikbaar stellen van de ITSM-oplossing wordt uitgesteld of vertraagd, is Opdrachtgever gerechtigd tot wijziging van de tijdstippen, dan wel wijziging van het aantal personeelsleden te verlangen dat aan de Opleiding deelneemt.

9.3. Voortbrenging van (onderdelen) van de ITSM-oplossing

Voortbrenging van Programmatuur en systeemonderdelen van de ITSM-oplossing gebeurt op basis van 'Security by Design'-principes. Beveiliging is vanuit het ontwerp geborgd, op een correcte manier geïmplementeerd en zowel proces als output wordt regelmatig geëvalueerd.

Als er open sourcecode wordt gebruikt dan is hier expliciet aandacht voor.

Dit is ook van toepassing op mobiele apps en de back-end daarvan. Bij Secure Software Development-processen kan gedacht worden aan ASVS en MASVS (zie website www.owasp.org of gelijkend).

GUE 74.	De gangbare principes rondom 'Security by Design' en 'Security by Default' zijn uitgangspunt voor het ontwerp en de ontwikkeling van de Programmatuur van de ITSM-oplossing ondersteund door een secure software development life-cycle.
---------	--

Webheaders zijn regels die voor een webapplicatie ingesteld kunnen worden richting de web browser. Met de juiste instellingen worden maatregelen geïmplementeerd die een webapplicatie veiliger kunnen maken. Denk hierbij bijvoorbeeld aan X-Frame-Options, X-Content-Type-Options, Content-Security-Policy en Referred-Policy. Zie voor meer informatie de website van OWASP Foundation.

Om te bepalen of de beveiliging via webheaders afdoende is geborgd, gebruikt de Belastingdienst de dienst 'Security Headers' (<https://securityheaders.com/>). Er moet minimaal een A-score behaald te worden. Zet 'Hide results' aan.

GUE 75.	Als de ITSM-oplossing webheaders toepast, dan voldoet de ITSM-oplossing aan bovenstaande alinea.
	Als de ITSM-oplossing geen webheaders toepast, dan kan op de GUE met NVT worden geantwoord.

Hoofdstuk 10. Onderhoud & Support

10.1. Onderhoud & Support

Opdrachtnemer is gedurende de looptijd van de Overeenkomst gehouden tot het leveren van Onderhoud & Support ten behoeve van ITSM-oplossing.

Service Level Agreement (SLA)

De Opdrachtgever sluit met de Opdrachtnemer een Service Level Agreement (SLA) af aangaande het te leveren Onderhoud & Support. De SLA bevat een beschrijving van de vastgestelde normen in de vorm van Service Levels.

UE 58.	De Inschrijver aan wie de opdracht voorlopig is gegund, levert tijdens de verificatiefase op basis van de inhoud van Bijlage A 'Specificaties van de opdracht, versie 1.2' gespecificeerde Service Levels, een concept SLA op. De SLA beschrijft in elk geval de wijze waarop door Opdrachtnemer invulling wordt gegeven aan derde lijns Onderhoud & Support.
--------	---

In het SLA moeten, naast alle in de aanbestedingsstukken gevraagde Service Levels, de navolgende onderwerpen benoemd worden:

- Doel en scope van het document;
- Benoeming partijen, verantwoordelijkheden en werkingsgebied;
- Aanvang, looptijd, wijzigingsbeleid, vaststelling en ondertekening;
- Gerelateerde documenten;
- Beschrijving en scope van de dienstverlening;
- In het kader van informatiebeveiliging:
 - Servicedesk (melding en oppakken prio 1-security incidenten, datalekken);
 - Change-en releasemanagement (waaronder security patches en significante juridische en infrastructurele wijzigingen);
 - Continuïteit (BCM);
 - Securitymanagement;
 - Incident- en problemmanagement;
 - Audits, beveiligingstesten (A&P-testen, vulnerability scans) en continuïteitstesten (Back-up & Restore, Calamiteitentests);
 - Stekkermanfaat;
 - Monitoring, alerting en logging.
- Rapportage

Rapportage

Opdrachtnemer rapporteert maandelijks in ieder geval over het volgende:

- KPI opgeloste beveiligingsincidenten/-problems.
- Status, voortgang en afhandeling van openstaande en opgeloste vragen, beveiligingsincidenten, -problems en -verbetervoorstellen. Hierbij wordt aangegeven: datum ontvangst, datum in behandeling, verwachte opleverdatum en datum afgevoerd.
- Cumulatieve rapportage (minimaal 14 maanden) over bovenstaande voor trend-analyse.

Opdrachtnemer rapporteert jaarlijks in ieder geval over het volgende:

- Wijziging van de Statement of Applicability en/of ISO27001-certificering (of gelijkwaardig).

Opdrachtnemer communiceert jaarlijks de data wanneer onderstaande aspecten plaatsvinden:

- Audits;
- Beveiligingstesten (A&P-testen, kwetsbaarheidscans);
- Continuïteitstesten (Back-up & Restore, Calamiteitentest)

UE 59.	Opdrachtnemer stelt in overleg met de Aanbestedende dienst na gunning én binnen 3 maanden na de ingangsdatum van de Overeenkomst, op basis van het ingediende concept SLA, de definitieve SLA op waarin alle, in de aanbestedingsstukken gevraagde onderwerpen zijn opgenomen.
--------	--

UE 60.	De SLA wordt binnen 3 maanden na het tekenen van de Overeenkomst tussen Opdrachtnemer en Opdrachtgever vastgesteld. Na vaststelling van de versie 1.0 zal deze jaarlijks worden onderhouden als er wijzigingen in de SLA optreden. De versienummering geeft aan welke SLA de laatste versie is. De SLA zal na ondertekening door Partijen als een Bijlage aan de Overeenkomst worden toegevoegd.
UE 61.	Opdrachtnemer verplicht zich om in overleg met de Opdrachtgever een Governance te beschrijven.
UE 62.	Opdrachtnemer stelt contactpersonen beschikbaar voor: - Een vast aanspreekpunt voor SLA-aspecten; - Een vast specifiek aanspreekpunt voor afhandelen van beveiligingsonderwerpen; - Een vast specifiek aanspreekpunt voor afhandelen van privacy gerelateerde onderwerpen. Dit mag één en dezelfde persoon zijn.

Dossier Afspraken & Procedures (DAP)

In het DAP moeten, naast alle in de aanbestedingsstukken gevraagde onderwerpen, de navolgende onderwerpen benoemd worden

- Doel en scope van het document;
- Benoeming partijen, verantwoordelijkheden en werkingsgebied;
- Aanvang, looptijd, wijzigingsbeleid, vaststelling;
- Standaard- en escalatiecommunicatiestructuur met rollen en contactgegevens;
- Afspraken en procedures (beveiligings- en privacy incidenten) betreffende:
 - Beschikbaarheid van de Servicedesk;
 - Prioriteriteitsbepaling, reactietijd en oplossingstijd;
 - Melding en afhandeling van incidenten, problems, common vulnerability disclosures en privacy gerelateerde incidenten;
 - Release-en patchmanagement. Releasekalender;
 - Aanvraag, uitvoering en afhandeling van audits, beveiligingstesten (A&P-test en Vulnerabilityscan) en continuïteitstesten (Back-up & Restore, Calamiteitentest);
 - Beschikbaar stelling en afhandeling van rapportages van audits, beveiligingstesten en continuïteitstesten van de Opdrachtnemer;
 - Afhandeling van Stekkermanaat (uitvoeren, herstellen);
 - Afspraken rond monitoring, logging en alerting;
 - Wijzigingen van beveiligingsstandaards (Forum van Standaardisatie);
 - Beschikbaar stellen van SLA-rapportages (SNR);
 - Beschikbaarstelling en gebruik van productiegegevens (Stekkermandaat, Retransitie) buiten de Productie-omgeving;
 - Opstellen Verbeterplan;
 - Wijzigingen die de juridische status (bijvoorbeeld rond de AVG) wijzigen;
 - De procedures met betrekking tot Recovery Time Objective en Recovery Point Objective.

UE 63.	Opdrachtnemer stelt in overleg met de Aanbestedende dienst na gunning én binnen 3 maanden na de ingangsdatum van de Overeenkomst een DAP op waarin alle, in de aanbestedingsstukken gevraagde onderwerpen, zijn opgenomen.
UE 64.	In het DAP is beschreven wat de procedure is hoe om gaan met wijzigingen bij het Forum Standaardisatie met betrekking tot (verplichte) Open Standaarden.

10.1.1. Service Levels

UE 65.	Opdrachtnemer neemt op verzoek deel aan een strategisch-, tactisch- en/of operationeel overleg deel.
--------	--

10.1.1.1. Beschikbaarheid

PI	Service Level
Beschikbaarheid 7x24x365	Minimaal 99,5 % per jaar ²

Tabel 2 Beschikbaarheid

Het is belangrijk te weten welke maatregelen getroffen zijn om eventuele onbeschikbaarheid te voorkomen én hoe snel de Gegevens beschikbaar zijn dan wel de ITSM-oplossing weer volledig operationeel kan zijn, indien de onbeschikbaarheid toch groter mocht zijn dan gepland. Het gaat hierbij dus niet om de operationele beschikbaarheidseisen (waar het vooral draait om wanneer de ITSM-oplossing wel of niet te gebruiken is), maar om de excepties als het mis gaat (Calamiteiten en Back-up & Restore). Verwacht wordt dat de ITSM-oplossing bij onbeschikbaarheid binnen bepaalde termijnen weer beschikbaar is zonder verlies van integriteit en vertrouwelijkheid.

UE 66.	De ITSM-oplossing voldoet ten minste aan de Beschikbaarheid zoals opgenomen in Tabel 2 Beschikbaarheid.
--------	---

10.1.1.2. Helpdesk en Incidentmanagement

Incidenten kunnen met drie verschillende prioriteiten aangemeld worden. Aan elk Incident, ongeacht de vermoedelijke oorzaak van een Incident, wordt een prioriteit toegekend op basis van Impact en Urgentie. Naast de door de Opdrachtgever gemelde Incidenten aan de Helpdesk van de Opdrachtnemer worden tevens de meldingen die door middel van het automatisch uitbellen/signaleren van de Oplossing bij de Opdrachtnemer beschouwd als daadwerkelijke Incidenten.

Impact	
Hoog	Een Incident heeft of kan ernstige gevolgen hebben voor • Eén of meer bedrijfsprocessen die de burger en/of het bedrijf direct raken, en/of • Eén of meer fabriekstaken voor (massale) gegevensverwerking en/of • De Informatiebeveiliging en/of • Het imago van de Opdrachtgever en/of • Onacceptabele hoge kosten.
Laag	• Overige situaties
Urgentie	
Hoog	Een Incident • Beïnvloedt kwaliteit van functies/Beschikbaarheid/beveiliging en/of • Brengt integriteit van de Gegevens in het geding en/of • Treedt op tijdens piektijd/-periode van het bedrijfsproces en/of • Brengt uiterste verzenddatum van klantbescheiden in gevaar en/of • Verstoort de communicatie met de klanten van de Opdrachtgever en/of • Er geen Workaround mogelijk is en/of • De verwerking kan niet worden uitgesteld en/of • De schade is al een feit of zal dat zijn binnen 24 uur.
Laag	• Overige situaties
Prioriteit	
	• Impact Hoog/ Urgentie Hoog geeft Prio 1; • Impact Hoog/ Urgentie Laag geeft Prio 2; • Impact Laag/ Urgentie Hoog geeft Prio 2; • Impact Laag/ Urgentie Laag geeft Prio 3.

Tabel 3 Impact, Urgentie en Prioriteit

² Toelichting: voor gepland Onderhoud geldt maximaal 2 uur per maand.

PI	Prioriteit	Service Level	Norm
Openstelling Helpdesk (Portal of email)	Incidenten	7 x 24 uur	99,9 % per jaar
Openstelling Helpdesk (Telefonisch)	Incidenten	07:00 – 21:00 uur	100% op Werkdagen
Openstelling Helpdesk (Telefonisch, Portal of email)	Beveiligingsincidenten/ (potentiële) Datalekken	7 x 24 uur	100% voor Prio 1
Service requests		Werkdagen van 08:00 – 17:00 uur	100%
REACTIETIJD			
Reactietijd	Prio 1	30 minuten	100%
Reactietijd	Prio 2	60 minuten	100%
Reactietijd	Prio 3	8 uur	100%
Reactietijd	Service request	1 Werkdag	100%
STREEFTIJD VOOR OPLOSSING			
Oplostijd	Prio 1	8 uur	100%
Oplostijd	Prio 2	1 Werkdag	100%
Oplostijd	Prio 3	5 Werkdagen	100%
STREEFTIJD VOOR HERSTEL			
Hersteltijd	Prio 1	2 Werkdagen	98%
Hersteltijd	Prio 2	5 Werkdagen	95%
Hersteltijd	Prio 3	10 werkdagen	90%
Recovery Time Objective (RTO)	n.v.t.	8 klokuren	n.v.t.
Recovery Point Objective (RPO)	n.v.t.	Maximaal 4 klokuren verlies aan Gegevens	n.v.t.

Tabel 4 Service Levels Helpdesk en Incidentmanagement

UE 67. Ten aanzien van de Openstelling van de Helpdesk wordt ten minste voldaan aan de Service Levels zoals opgenomen in Tabel 4 Service Levels Helpdesk en Incidentmanagement.

UE 68. Opdrachtnemer geeft ten aanzien van de afhandeling van beveiligingsincidenten en (potentiële) Datalekken minimaal het volgende aan:

- De omvang;
- De verwachte consequenties voor de Belastingdienst;
- Getroffen en/of te nemen maatregelen.

De procedures hiervoor worden in een DAP beschreven.

GUE 76. De voertaal op de Helpdesk is Nederlands en/of Engels.

GUE 77. Het is mogelijk om Events, Incidenten en/of Problems via meerdere kanalen, bijvoorbeeld via de Self service portal of mail, aan te melden.

10.1.1.3. Release – en Patch management

GUE 78. Inschrijver heeft Patchmanagement ingericht.
De bedrijfsvoering is zodanig ingericht dat technische kwetsbaarheden adequaat worden ontdekt, geëvalueerd en geadresseerd.

UE 69. Opdrachtnemer informeert Opdrachtgever over nieuwe Releases en Patches ten behoeve van het optimaal gebruik van de ITSM-oplossing en de daarbij verwachte Impact voor Opdrachtgever.

	In het DAP worden afspraken gemaakt op welk tijdstip Opdrachtgever hierover geïnformeerd wordt.
GUE 79.	Tijdens het doorvoeren van Releases en Patches blijft de ITSM-oplossing beschikbaar.
UE 70.	Opdrachtnemer levert voorafgaand aan de Release ten behoeve van het optimaal gebruik van de ITSM-oplossing de releasenotes op.
UE 71.	Gedurende de Overeenkomst is er voor Opdrachtgever een actuele Roadmap van de ITSM-oplossing beschikbaar.
UE 72.	Opdrachtnemer zorgt ervoor dat de nieuwe ontwikkelingen binnen IT4IT en ITIL worden doorgevoerd in de ITSM-oplossing. Deze informatie is terug te zien in de Roadmap.
UE 73.	Opdrachtnemer informeert Opdrachtgever minimaal 1 jaar over de datum wanneer delen van de ITSM-oplossing EOD en/of EOL en/of EOS zijn. In het DAP worden afspraken gemaakt op welk tijdstip Opdrachtgever hierover geïnformeerd wordt.
GUE 80.	De ITSM-Oplossing beschikt over een geautomatiseerd voortbrengingsmechanisme t.b.v. Functionele Inrichtingen. Voorbeeld: In de Testomgeving wordt bijvoorbeeld een workflow ontwikkelt; deze kan dan geautomatiseerd worden voortgebracht naar de productie omgeving.

10.1.1.4. Verbeterplan

UE 74.	Indien de ITSM-oplossing voor een periode van drie (3) maanden niet voldoet aan één of meerdere Service Levels levert Opdrachtnemer hiervoor een Verbeterplan, inclusief een bijbehorend implementatievoorstel, aan bij de Opdrachtgever. Het verbeterplan moet leiden tot een situatie waarbij de Service Levels wel worden gerealiseerd. Het Verbeterplan wordt binnen tien (10) Werkdagen na verzoek van de Opdrachtgever opgeleverd. Toepassing van het Verbeterplan laat de overige rechten van Opdrachtgever onverlet, waaronder die op schadevergoeding.
--------	---

10.1.2. Rapportage

UE 75.	Opdrachtnemer levert maandelijks een Service Level rapportage op aan de Opdrachtgever met minimaal de volgende inhoud: • Helpdesk: Reactietijden per Prio; • Beschikbaarheid; • KPI Incident management; • KPI Helpdesk; • Performance rapportage; • Licentie- en/of Subscription gebruik.
UE 76.	Opdrachtnemer overlegt minimaal eenmaal per jaar aan Opdrachtgever het schriftelijk bewijs dat zij aan haar verplichtingen heeft voldaan betreffende het nemen van de gestelde securitymaatregelen en de geëiste verbeteracties (zoals gedefinieerd in dit document). Als bewijs hiervoor kunnen certificeringen en/of uitkomsten van kwetsbaarheidsonderzoeken, A&P testen en/of calamiteitstesten dienen.

10.2. Factureren en bestellen

Als leverancier bent u verplicht elektronisch te factureren

Wij zijn als overheid vanaf november 2018 verplicht om e-factureren te implementeren. Dit is vastgelegd in de EU-Richtlijn Elektronische facturering bij overheidsopdrachten (2014/55/EU). De Rijksoverheid werkt sinds 1 januari 2017 bij nieuwe overeenkomsten met e-facturering.

Manieren van e-factureren

Ondernemers die goederen of diensten aan de Rijksoverheid leveren en een e-factuur willen sturen, kunnen dat op verschillende manieren doen,

- Via een DigiPoort aansluiting;
- Via het netwerk Peppol;
- Via het leveranciersportaal.

Bekijk de video op de website: [Home | Helpdesk e-factureren \(helpdesk-efactureren.nl\)](https://www.helpdesk-efactureren.nl/).

DigiPoort

De DigiPoort is een technische voorziening die beheerd wordt door Logius en die het mogelijk maakt om diverse elektronische berichten (waaronder facturen) met de Rijksoverheid uit te wisselen. Meer informatie over berichtenuitwisseling via de DigiPoort vindt u op [Handleiding Aansluiten op Digipoort voor Bedrijven | Logius](https://www.logius.nl/nl/onderwerpen/digipoort)

Peppol

Peppol is een digitale infrastructuur gebaseerd op open standaarden voor het eenvoudig en veilig uitwisselen van e-facturen en andere elektronische berichten. Met Peppol kunt u e-facturen rechtstreeks versturen vanuit uw boekhoudsysteem of e-facturen versturen via een (commercieel)Peppol-portaal. Peppol is de nieuwe EU standaard voor elektronisch berichtenverkeer met de overheid. Meer informatie over Peppol vindt u op www.peppolautoriteit.nl/

Leveranciersportaal

U kunt ook gebruik maken van het e-factuurportaal van de Rijksoverheid, het leveranciersportaal. Op dit portaal kunt u e-facturen versturen en inkooporders of tijdkaarten ontvangen indien het departement dit ondersteunt. Het Rijk bevindt zich in een transitiefase wat betreft het leveranciersportaal. Het huidige leveranciersportaal van DigiInkoop wordt vervangen. U wordt tijdig geïnformeerd over de overgang naar het nieuwe leveranciersportaal.

UE 77.	De Opdrachtnemer voldoet, conform Bijlage 5 Bijsluit e-factureren juli 2022, aan de vereisten van e-facturatie via het leveranciersportaal of een geautomatiseerde koppeling met de DigiPoort (toekomstig E-procurementpoort) of het Peppol netwerk met daarin de referentie naar de inkooporder en de inkooporderregel. Zie ook https://www.helpdesk-efactureren.nl/bijsluiter voor de meest actuele informatie.
UE 78.	Kosten die voortkomen uit het realiseren van de koppeling voor elektronische berichten uitwisseling met de Rijksoverheid worden gedragen door de Opdrachtnemer.
UE 79.	Opdrachtnemer vermeldt het inkoopordernummer als referentie op elke pakbon en factuur aan Opdrachtgever. Zonder dit Inkoopordernummer kan Opdrachtgever de levering of de factuur weigeren.
UE 80.	Opdrachtnemer is verantwoordelijk voor de implementatie aan haar zijde. Op verzoek van Opdrachtgever kunnen wijzigingen in het implementatieplan en/of implementatie worden aangebracht die invloed hebben op het bestelproces. Hieronder valt in ieder geval het inzetten van extra expertise.
UE 81.	Opdrachtnemer accepteert dat er gedurende de looptijd van de Overeenkomst nieuwe-/verbeterde Releases van het leveranciersportaal in gebruik genomen kunnen worden.

10.3. Kaders voor (re)transitie

10.3.1. Inleiding

In geval van (tussentijdse) beëindiging of afloop van de Overeenkomst van de ITSM-oplossing, dient de Opdrachtnemer te allen tijde alle medewerking te verlenen aan een gecontroleerde en projectmatige overdracht aan een opvolgende opdrachtnemer of Opdrachtgever en daarmee alle Documentatie, Gegevens en informatie te verstrekken die nodig zijn voor een goede overdracht.

De termijn waarbinnen de Retransitie dient te worden afgerond zal tussen Opdrachtnemer en Opdrachtgever worden overeengekomen.

Hierbij zal in ieder geval het maximaal aantal uren of dagen benodigd voor de Retransitie worden overeengekomen tussen de Opdrachtnemer en Opdrachtgever. De geldende Prijs is gebaseerd op de aangeboden Prijzen voor Additionele diensten in de vorm van Consultancy, zoals ingevuld in Bijlage VIII Prijzenformulier versie 1.1.

10.3.2. Documentatie en Gegevens(overdracht)

UE 82.	Zodra Partijen bekend zijn met het feit dat de Overeenkomst om welke reden dan ook eindigt of wordt beëindigd, waaronder begrepen opzegging en ontbinding, inventariseren Partijen gezamenlijk welke assistentie van Opdrachtnemer, tegen marktconforme tarieven, noodzakelijk is voor een succesvolle Retransitie waarbij de continuïteit van de Prestatie gewaarborgd blijft. Hierbij wordt, indien noodzakelijk, een Retransitieplan opgesteld door de Partijen, waarvoor de (Uitvoerings)eisen uit paragraaf 10.3 en volgende leidend zijn.
UE 83.	Opdrachtnemer verleent volledige medewerking aan de Retransitie en verstrekt daarbij alle relevante Documentatie aan Opdrachtgever c.q. opvolgende opdrachtnemer.
UE 84.	Aanlevering van de Documentatie gebeurt via een beveiligde verbinding. Opdrachtgever draagt zorg voor deze verbinding.
UE 85.	De ter beschikking gestelde Gegevens dienen te zijn voorzien van een zodanige functionele - en technische beschrijving dat in de toekomst een datamigratie naar een nieuwe oplossing kan plaatsvinden zonder verdere tussenkomst van de Opdrachtnemer.
UE 86.	Opdrachtnemer verstrekt op verzoek van de Opdrachtgever gewenste Gegevens in een voor de Opdrachtgever bruikbaar (digitaal) formaat voor verdere verwerking. De procedure hiervoor moet worden beschreven in een DAP met de Belastingdienst.
UE 87.	Na ontvangst van bevestiging dat de Gegevens in goede orde zijn ontvangen, zal de Opdrachtnemer overgaan tot vernietiging van onder hem bevindende Gegevens, waarbij de vernietigingshandelingen gedocumenteerd zullen worden.
UE 88.	Opdrachtnemer zorgt dat binnen één (1) maand na afloop van de Retransitie, alle Gegevens in verband met deze Overeenkomst van haar systemen zijn verwijderd, zodat de vertrouwelijkheid van deze Gegevens gewaarborgd blijft.
UE 89.	Op eerste verzoek van Opdrachtgever overlegt Opdrachtnemer een door een onafhankelijk IT-auditor of accountant gecertificeerde verklaring van vernietiging waaruit blijkt dat alle Gegevens in verband met deze Overeenkomst zijn gewist. In de verklaring is aangegeven hoe de Gegevens zijn vernietigd (bijvoorbeeld: twee keer overschreven met vaste Gegevens en één keer met random gegevens of met Programmatuur zoals beschreven op https://www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducten/geevalueerde-producten . De procedure moet worden beschreven in het DAP.
UE 90.	Naar de Belastingdienst herleidbare domeinnamen en URL's worden onbeschikbaar gemaakt op het internet en domeinnamen worden –zo mogelijk– overgedragen aan de Belastingdienst.
UE 91.	Hergebruik van deze domeinnamen en URL's (n.a.v. UE 90) is niet toegestaan zonder nadrukkelijke toestemming van de Opdrachtgever.

10.3.3. (Proces)afspraken Retransitiefase

Om te waarborgen dat de Retransitie op een efficiënte en ongestoorde wijze plaatsvindt, zal de Opdrachtnemer in ieder geval voldoen aan de volgende uitvoeringseisen:

UE 92.	Bij overgang naar een nieuwe opdrachtnemer moet de Prestatie voor een periode van minimaal 6 maanden tegen gelijkblijvende condities (naar rato), voor Opdrachtgever beschikbaar blijven.
UE 93.	Opdrachtnemer houdt voldoende gekwalificeerd personeel beschikbaar voor de Retransitie.
UE 94.	Opdrachtnemer verleent medewerking aan een Audit betreffende de inhoud en de kwaliteit van de informatie die Opdrachtnemer in het kader van Retransitie beheerd.
UE 95.	Opdrachtnemer dient inzage te geven in de gebruikte middelen en processen tijdens de periode van Retransitie.
UE 96.	Opdrachtnemer dient onder meer de verbindingen te verbreken en eventuele Subscriptions te verstrekken ten aanzien van de ITSM-oplossing die noodzakelijk zijn om de omgeving in stand te houden/te blijven beheren.